

THUNDERBIRD, ENIGMAIL Y OPENPGP PARA WINDOWS - CORREO ELECTRÓNICO SEGURO

Publicado 10 August 2016

TABLA DE CONTENIDO

- Lectura requerida
- Qué obtendrás de esta guía
- 1. Introducción a Thunderbird
- 2. Instalar y configurar Thunderbird
- 3. Mejorar la seguridad y uso de Thunderbird
- 4. Enviar y recibir mensajes encriptados
- PREGUNTAS FRECUENTES

Mozilla Thunderbird es un software libre y de código abierto que te permite intercambiar y almacenar correo electrónico para múltiples cuentas con múltiples proveedores de servicio. **Enigmail** y **GnuPG** mejoran la seguridad y privacidad de tu correo electrónico agregando respaldo para encriptación integral para OpenPGP a **Thunderbird**. También te permiten firmar tus mensajes digitalmente y verificar las firmas digitales de otros.

LECTURA REQUERIDA

- [Mantén privada tu comunicación en línea \(../secure-communication\)](#)
- [Protege los archivos sensibles en tu computadora \(../secure-](#)

file-storage)



(<https://www.mozilla.org/thunderbird/>)

PROJECT WEBSITE ([HTTPS://WWW.MOZILLA.ORG/THUNDERBIRD/](https://www.mozilla.org/thunderbird/))

DOWNLOAD THUNDERBIRD ([HTTPS://WWW.MOZILLA.ORG/THUNDERBIRD](https://www.mozilla.org/thunderbird/))

GPG4WIN 2.3.1. ([HTTPS://WWW.GPG4WIN.ORG/](https://www.gpg4win.org/))

ENIGMAIL 1.9.2. ([HTTPS://WWW.ENIGMAIL.NET/DOWNLOAD/](https://www.enigmail.net/download/))

Versión: Thunderbird 45.1.1.

Licencia: Software libre y de fuente abierta/código abierto

Requisitos del sistema:

Microsoft Windows

Apple Mac OS X

GNU/Linux

QUÉ OBTENDRÁS DE ESTA GUÍA

- La capacidad de administrar múltiples cuentas de correo electrónico usando una sola herramienta
- La capacidad de leer y redactar mensajes mientras estás desconectado de internet
- La capacidad de enviar y recibir correos electrónicos encriptados
- La capacidad de firmar digitalmente tus correos electrónicos y autenticar correo firmado por otros

1. INTRODUCCIÓN A THUNDERBIRD

Thunderbird es un cliente de correo electrónico multiplataforma libre y de código abierto para enviar, recibir y almacenar correo electrónico. Un *cliente de correo electrónico* es una aplicación que te permite descargar y administrar tus mensajes — desde múltiples cuentas y múltiples proveedores — sin navegador.

Gnu Privacy Guard (GPG) es un software libre de código abierto capaz de encriptar, desencriptar y firmar digitalmente mensajes y archivos. También genera y administra las claves públicas y privadas necesarias para hacerlo.

Enigmail es un complemento de Thunderbird que te permite acceder a las funciones de encriptación y autenticación que ofrece GnuPG, que debe instalarse para que Enigmail funcione.

1.0 LO QUE DEBERÍAS SABER SOBRE THUNDERBIRD ANTES DE EMPEZAR

Necesitarás al menos una cuenta de correo electrónico para usar **Thunderbird**. Si quieres crear una nueva cuenta para usar con **Thunderbird**, consulta la guía de **RiseUp** ([../..../riseup/web](https://riseup.net/en/about/riseup/web)).

Como todos los *clientes de correo electrónico*, **Thunderbird** hace una copia de tus mensajes disponibles en tu computadora. Esto incluye los correos electrónicos que envías así como los que recibes. Como resultado, es particularmente importante que implementes encriptación de dispositivos

(como *BitLocker* (<http://windows.microsoft.com/en-us/windows-vista/bitlocker-drive-encryption-overview>) cuando decidas usar Thunderbird.

Thunderbird no puede proteger tu dispositivo si abres adjuntos maliciosos o haces clic en enlaces maliciosos. No abras adjuntos no solicitados y ten cuidado cuando hagas clic en enlaces que recibes por correo electrónico. Consulta la guía de **Proteger tu dispositivo de Software malicioso y hackers** ([../malware](http://securityinabox.org/es/guide/thunderbird/windows/malware)).

1.1 OTRAS HERRAMIENTAS COMO THUNDERBIRD

Thunderbird está disponible para **Microsoft Windows**, **Mac OS X** y **GNU/Linux**. Administrar de manera segura múltiples cuentas de correo electrónico es una tarea compleja, y te recomendamos Thunderbird para este fin. Sin embargo, si prefieres usar una herramienta alterna, te recomendamos las siguientes herramientas libres y de código abierto:

- **Claws Mail** (<http://www.claws-mail.org/>) disponible para GNU Linux y Microsoft Windows
- **Sylpheed** (<http://sylpheed.sraoss.jp/en/>) disponible para Mac OS X, GNU Linux y Microsoft Windows
- **K9 Mail and OpenKeychain** (<https://play.google.com/store/apps/details?id=org.sufficientlysecure.keychain&hl=en>) está disponible para Android
- **Mailpile** (<https://www.mailpile.is/>) tiene un **beta** disponible para GNU/Linux y Microsoft Windows (y debería estar disponible para Mac OS X en el futuro)

Las ventajas de seguridad de Thunderbird son significativas, particularmente cuando se le compara con alternativas comerciales como *Microsoft Outlook*.

2. INSTALAR Y CONFIGURAR THUNDERBIRD

2.1 INSTALAR THUNDERBIRD

Para instalar **Thunderbird**, sigue los pasos a continuación:

Paso 1. Navega a la página de descargas de **Thunderbird** en <https://www.mozilla.org/en-US/thunderbird> (<https://www.mozilla.org/en-US/thunderbird/>)



Figura 1: Página de descarga de Thunderbird

Paso 2. Haz clic en [Descargar gratis].

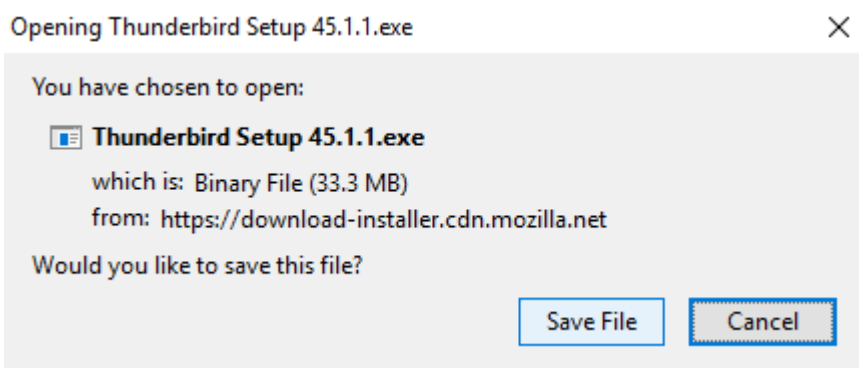


Figura 2: Descargar Thunderbird

Paso 3. Haz clic en [Guardar archivo] para empezar a descargar Thunderbird.

Paso 4. Haz clic derecho en el archivo descargado de Thunderbird y **elige [Abrir]** para extraer el archivo.

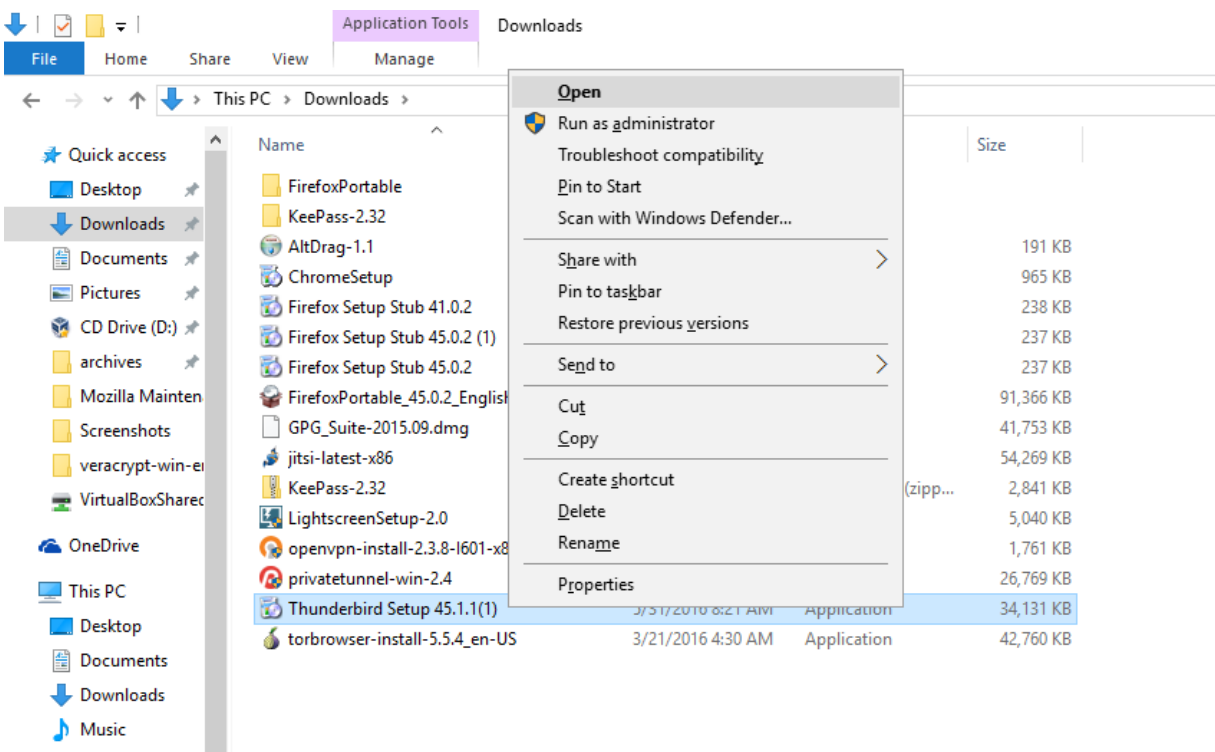


Figura 3: Abrir el archivo descargado de Thunderbird

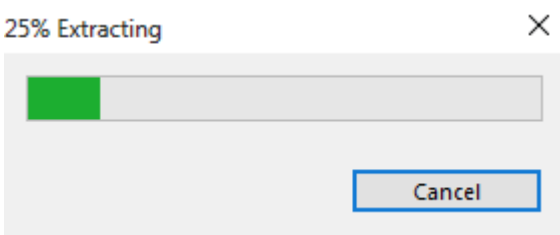


Figura 4: Extraer Thunderbird

Paso 5. Haz clic en [Siguiente] para empezar el proceso de configuración de Thunderbird.

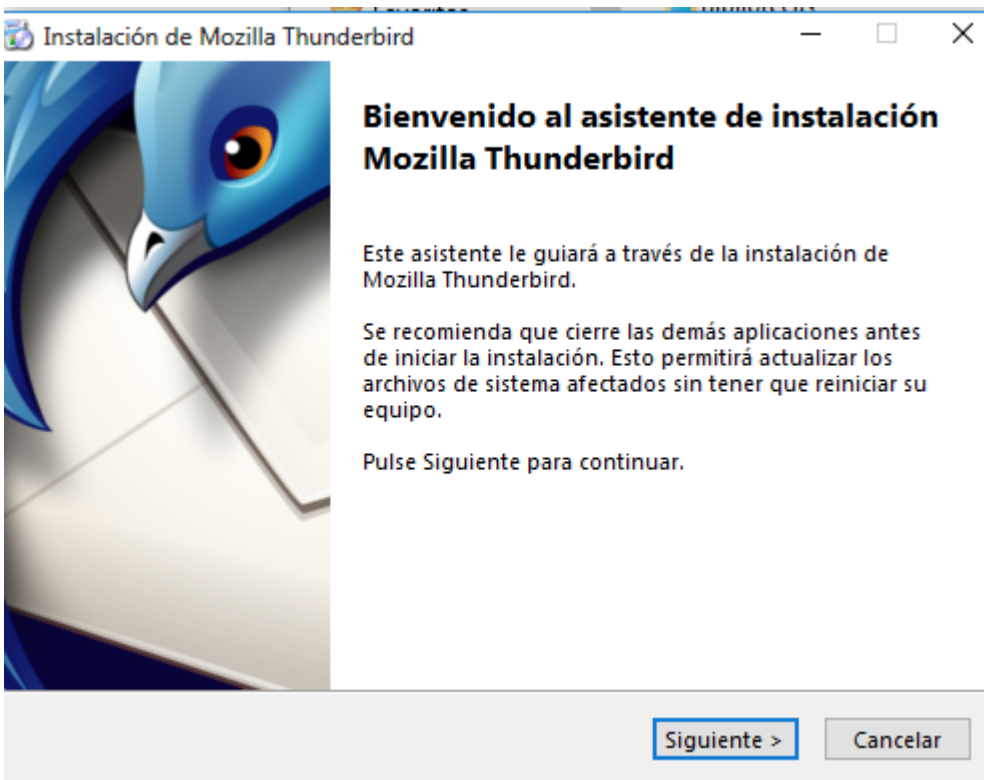


Figura 5: Ventana de configuración de Mozilla Thunderbird

Paso 6. Elige [Estándar] a través de la ventana de configuración de Mozilla Thunderbird.

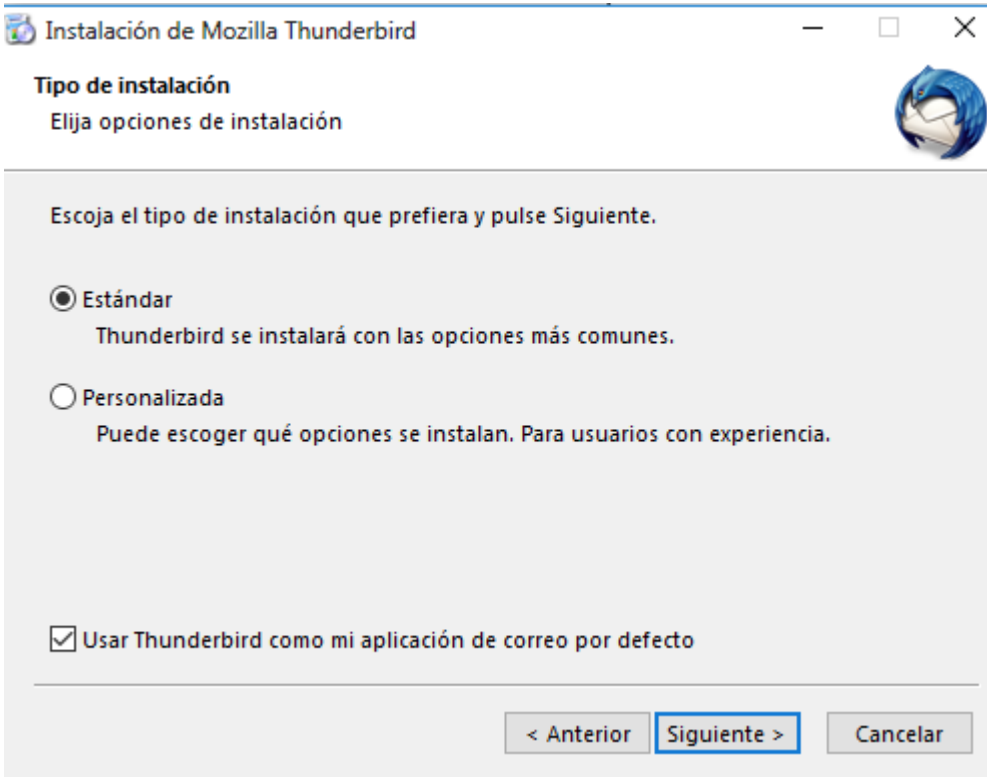


Figura 6: Opciones de configuración en la ventana de configuración de Mozilla Thunderbird

Paso 7. Marca [Usar Thunderbird como mi aplicación de correo por defecto] si prefieres que Thunderbird sea tu aplicación de correo por defecto.

Paso 8. Haz clic en [Siguiente] para continuar.

Paso 9. Haz clic en [Instalar] para empezar a instalar Thunderbird.

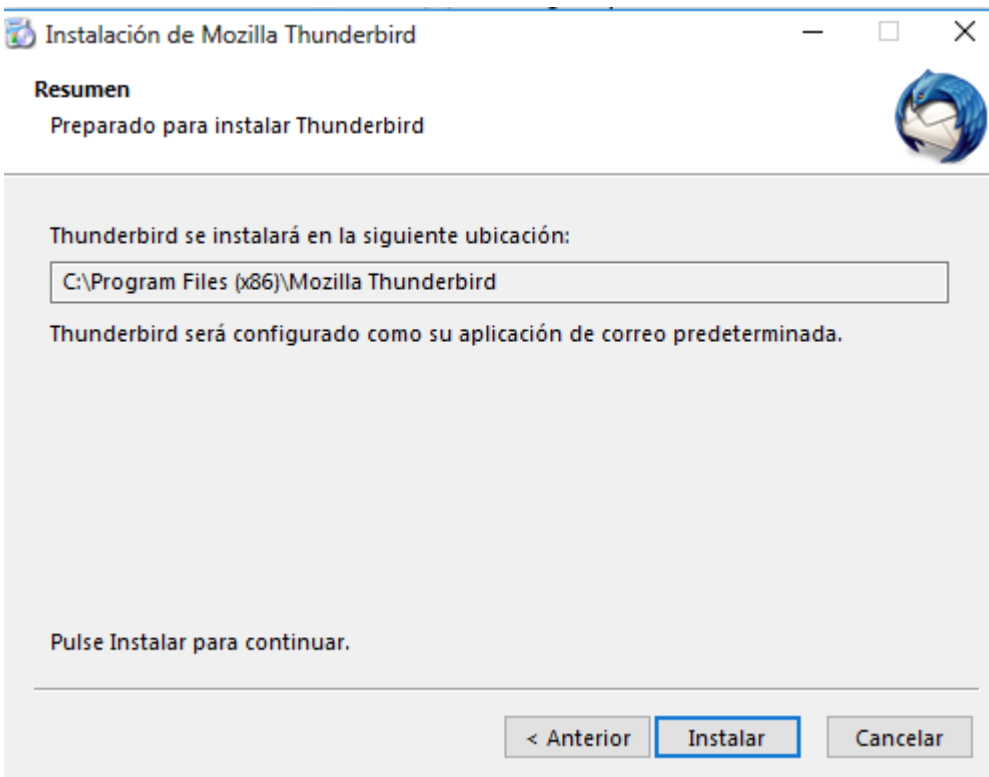


Figura 7: Empezar a instalar Thunderbird

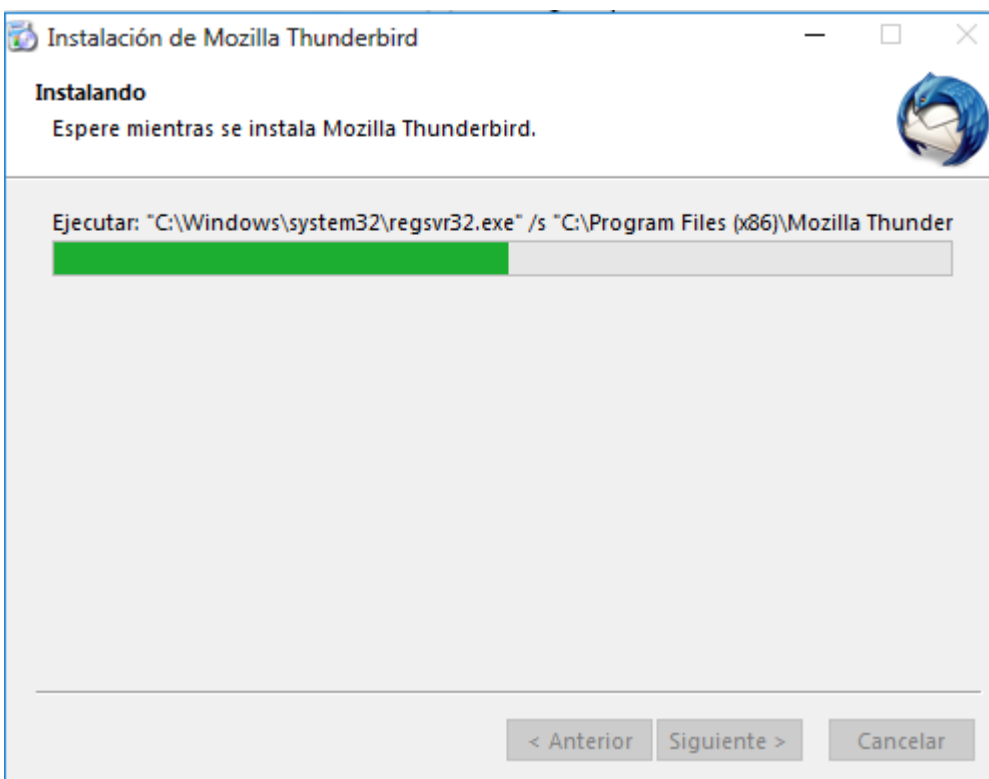


Figura 8: Instalar Thunderbird

Paso 10. Haz clic en [Terminar] para completar el proceso de instalación de Thunderbird.



Figura 9: Completar el proceso de instalación de Thunderbird

2.2 AGREGAR UNA CUENTA DE CORREO ELECTRÓNICO A THUNDERBIRD

Para agregar una cuenta de correo electrónico a **Thunderbird**, sigue los pasos a continuación.

Paso 1. Inicia Thunderbird y aparecerá la siguiente ventana (una vez que hayas configurado **[correo electrónico]** como opción por defecto):

Bienvenido a Thunderbird

¿Le gustaría tener una nueva dirección de correo?

Elena

Buscar

En colaboración con varios proveedores, Thunderbird puede ofrecerle una nueva cuenta de correo. Para ello, sólo tiene que rellenar su nombre y apellidos, o cualesquiera otras palabras que desee, en los campos anteriores.

☒  gandi.net

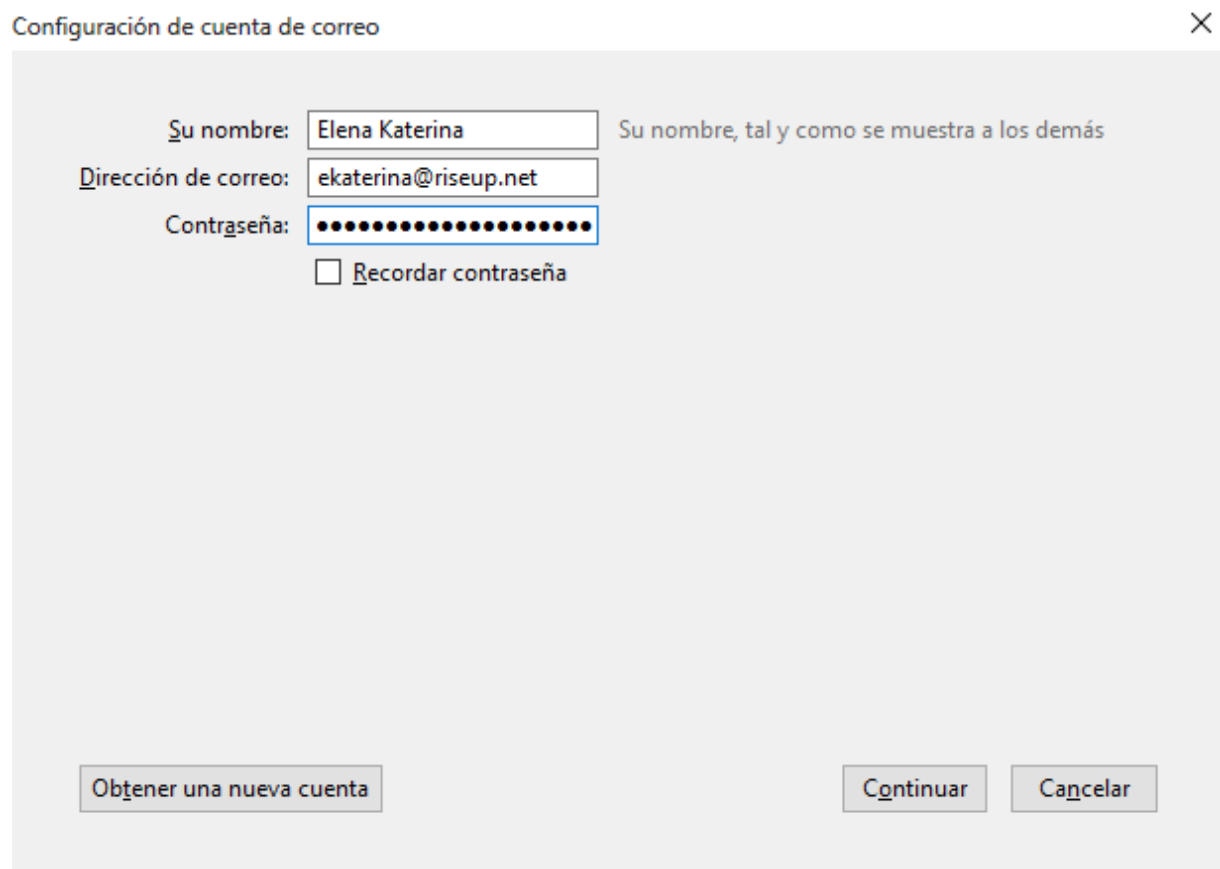
Los términos de búsqueda usados se envían a Mozilla ([política de privacidad](#)) y a los proveedores de correo independientes gandi.net ([Política de privacidad](#), [Términos del Servicio](#)) para encontrar direcciones de correo disponibles.

Saltarse esto y usar mi cuenta de correo existente

Creo que configuraré mi cuenta más tarde.

Figura 1: Primer inicio de Thunderbird

Paso 2. Haz clic en [Omitir esto y usar mi correo electrónico existente] para abrir la pantalla de *Configuración de cuenta de correo*.



Configuración de cuenta de correo

Su nombre: Elena Katerina Su nombre, tal y como se muestra a los demás

Dirección de correo: ekaterina@riseup.net

Contraseña: ●●●●●●●●●●●●●●●●

☐ Recordar contraseña

Obtener una nueva cuenta

Continuar Cancelar

Figura 2: Pantalla de configuración de cuenta de correo

Paso 3. Escribe el nombre, dirección de correo electrónico y contraseña que corresponda a la cuenta a la que deseas acceder usando Thunderbird.

Paso 4. Saca la marca del recuadro al lado de **[Recordar mi contraseña]**.

Paso 5. Haz clic en [Continuar]. Thunderbird revisará la configuración del servicio de correo electrónico que has consignado.

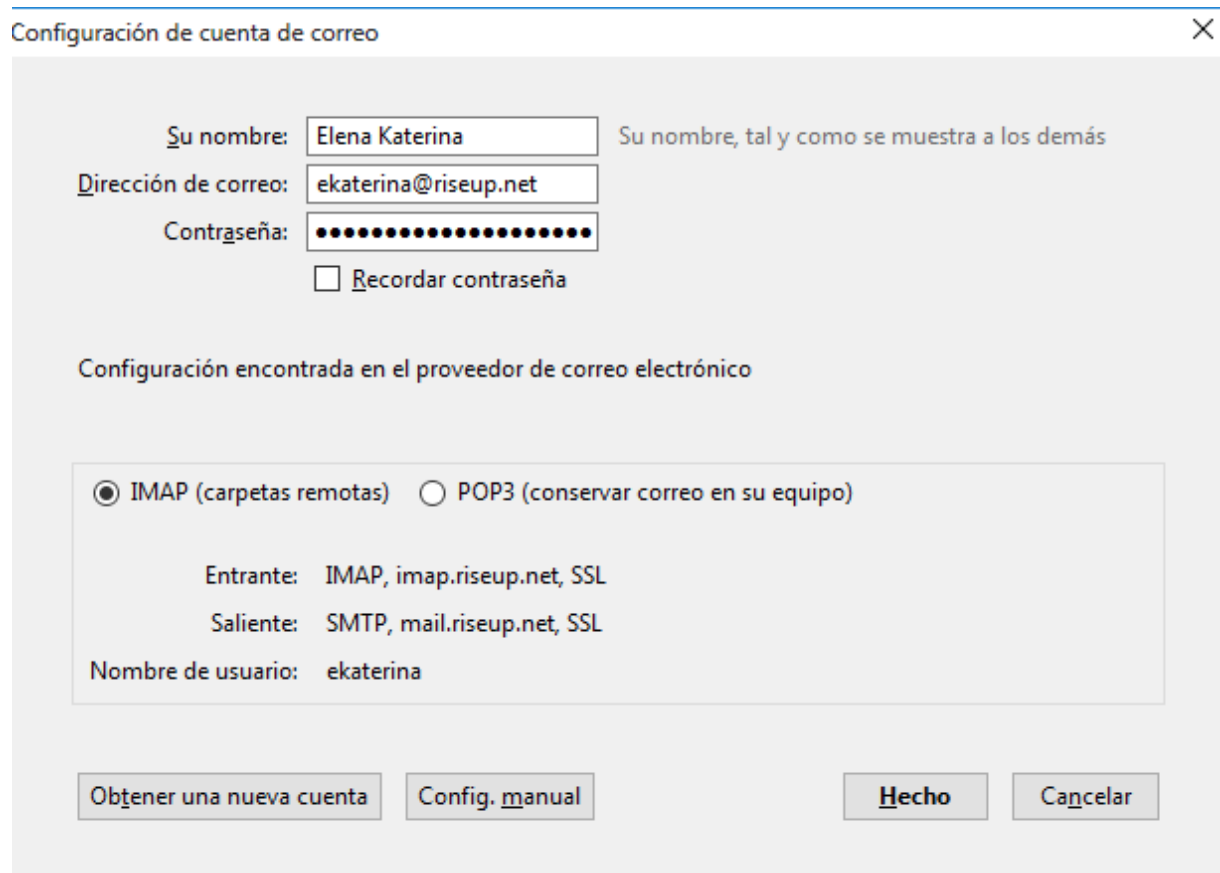


Figura 3: Thunderbird después de verificar la configuración de un servicio de correo electrónico

Probablemente quieras dejar elegidas las **"(carpetas remotas) de IMAP"**. *IMAP* almacena la copia maestra de las carpetas de tu correo electrónico (incluidas las carpetas de *Bandeja de entrada*, *Borradores*, *Plantillas*, *Enviados* y *Papelera*) en el servidor y hace una copia local en tu dispositivo. Esto te permite tener acceso a los mismos mensajes desde múltiples dispositivos mientras mantengas tus carpetas sincronizadas. (**POP**, de otro lado, recupera tus mensajes del servidor y los almacena en el primer dispositivo en el que se descargaron. *Esto no significa que realmente se hayan borrado del servidor*, pero sí hace mucho más difícil acceder a tu correo electrónico desde múltiples dispositivos.)

Importante: Asegúrate de que en la información *Entrante* y en la *Saliente* mostrada en la pantalla de abajo aparezca **SSL** (Secure Sockets Layer o seguridad de la capa de transporte) o **STARTTLS** (Start Transport Layer

Security o iniciar seguridad de transporte de capas). Cualquiera de los dos indica que tu proveedor de correo electrónico opera con encriptación básica.

Paso 6. Haz clic en [Listo] para crear tu cuenta y entrar a la interfaz principal de Thunderbird.

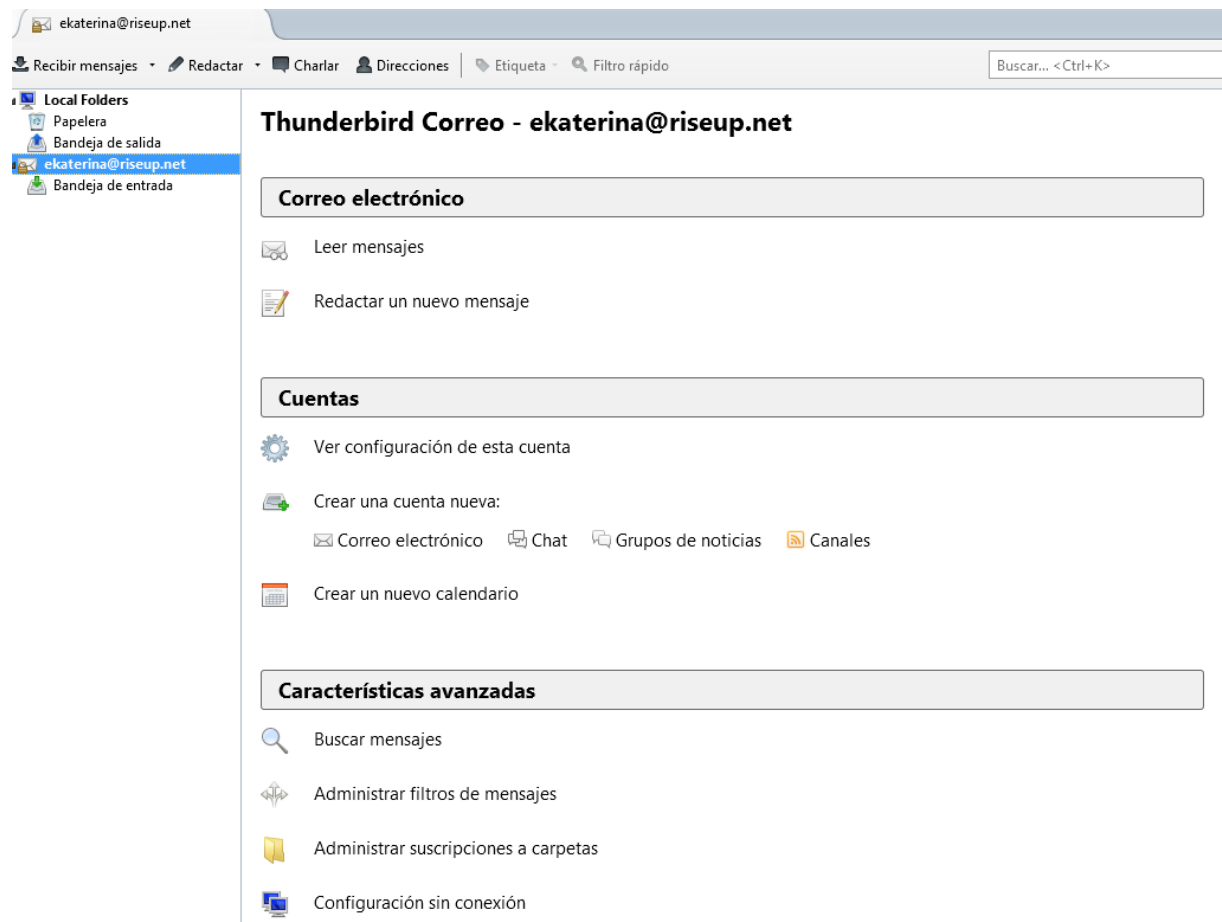


Figura 4: Interfaz principal de Thunderbird

Nota: Para agregar otra cuenta de correo electrónico, **haz clic** en *Archivo* en la barra de menú y **elige [Nuevo > Cuenta de correo existente]**. Después, simplemente repite los pasos anteriores.

Cada vez que inicies Thunderbird, deberás ingresar la contraseña para cada cuenta que hayas agregado.

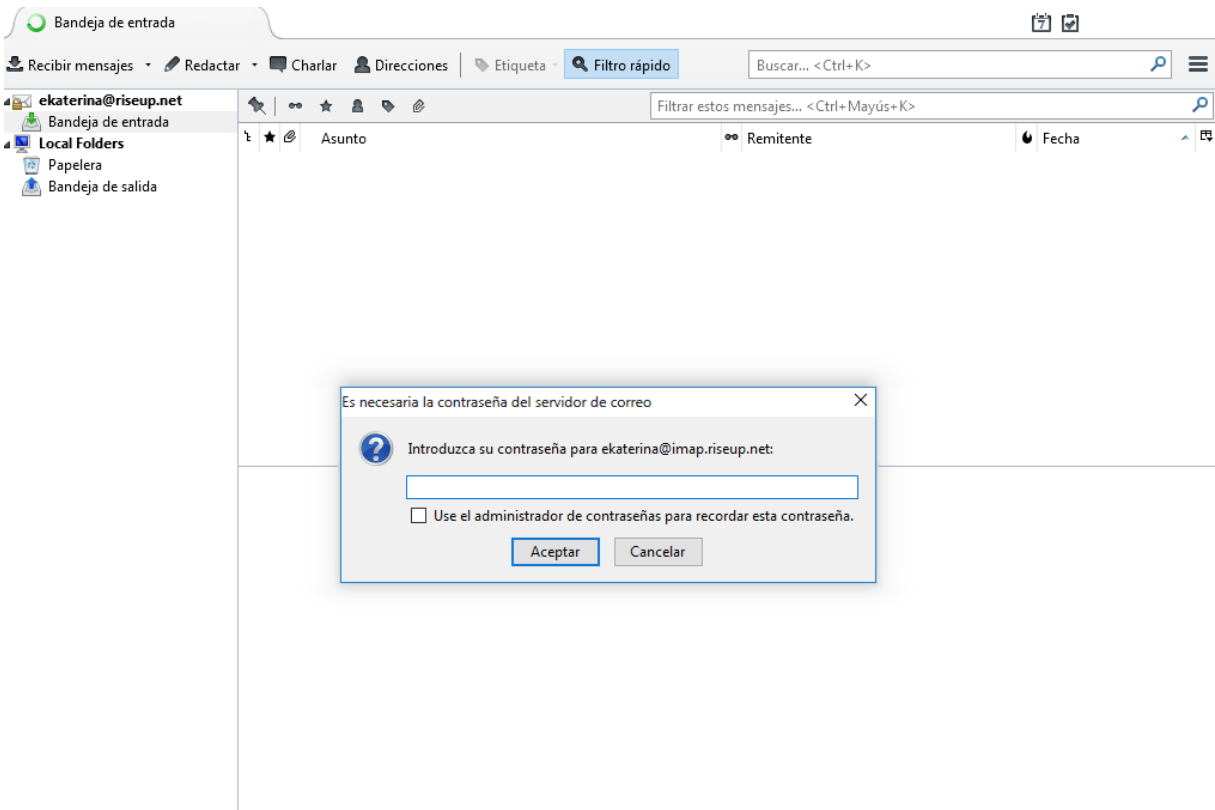


Figura 5: Pantalla Se requiere contraseña de servidor de correo

Paso 7. Escribe tu contraseña.

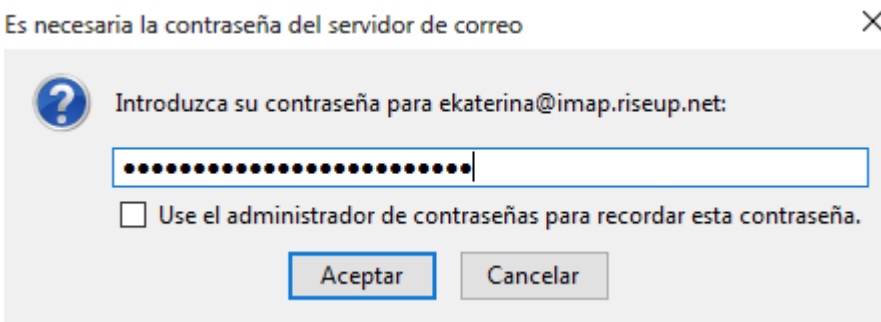


Figura 6: Consignar una contraseña en la pantalla de Se requiere contraseña de servidor de correo

Paso 8. Haz clic en [OK] para iniciar sesión en tu(s) cuenta(s) usando Thunderbird.

3. MEJORAR LA SEGURIDAD Y USO DE

THUNDERBIRD

Esta sección explica cómo configurar las preferencias de Thunderbird para ayudar a defender tu sistema de ataques que se originan en correos electrónicos. Para más información, ver [Protégete de Software malicioso y Hackers](https://securityinabox.org/en/guide/malware) (<https://securityinabox.org/en/guide/malware>).

3.1 INHABILITAR CORREO ELECTRÓNICO HTML

Thunderbird te permite incluir colores, fuentes, imágenes y demás formato en los correos electrónicos que escribes. Lo hace enviando mensajes que incluyen *HTML* — la misma tecnología que se usa en páginas web — en vez de usar solamente texto básico. También tiene la capacidad de mostrar mensajes HTML que otros te envían. Lamentablemente, ver correo electrónico en HTML puede exponerte a algunos ataques dirigidos contra navegadores para navegadores web. Y *escribir* correos electrónicos en HTML a veces impide que la encriptación GnuPG funcione correctamente.

Para mostrar correos electrónicos en HTML como texto plano, sigue los pasos a continuación:

Paso 1. Haz clic en  para mostrar el *Menú de Thunderbird*.

Paso 2. Elige [Ver > Cuerpo del mensaje como > Texto plano].

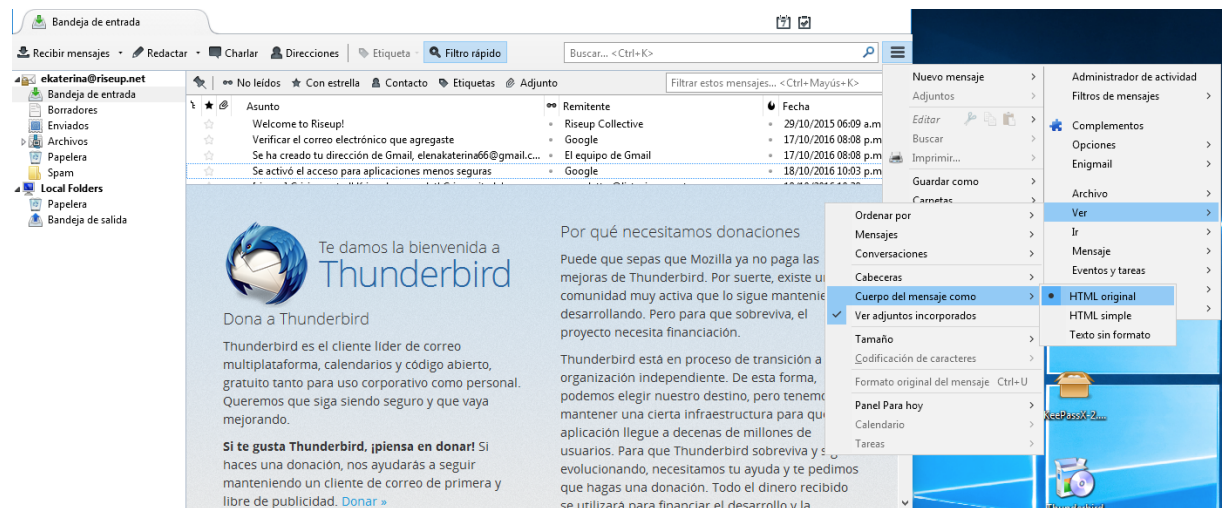


Figura 1: Inhabilitar mostrar el correo electrónico en HTML

Para escribir correo electrónico en texto plano, sigue los pasos a continuación:

Paso 1. Haz clic en  para mostrar el *Menú de Thunderbird*.

Paso 2. Elige [Opciones > Configuraciones de cuenta].

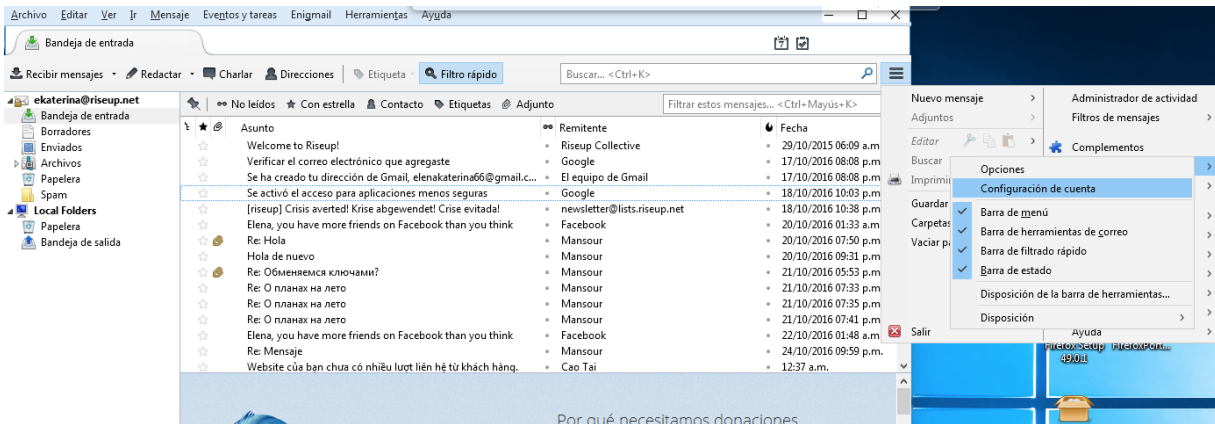


Figura 2: Elegir configuraciones de cuenta en Thunderbird

Paso 3. Elige [Redacción y Dirección] debajo de tu dirección de correo electrónico.

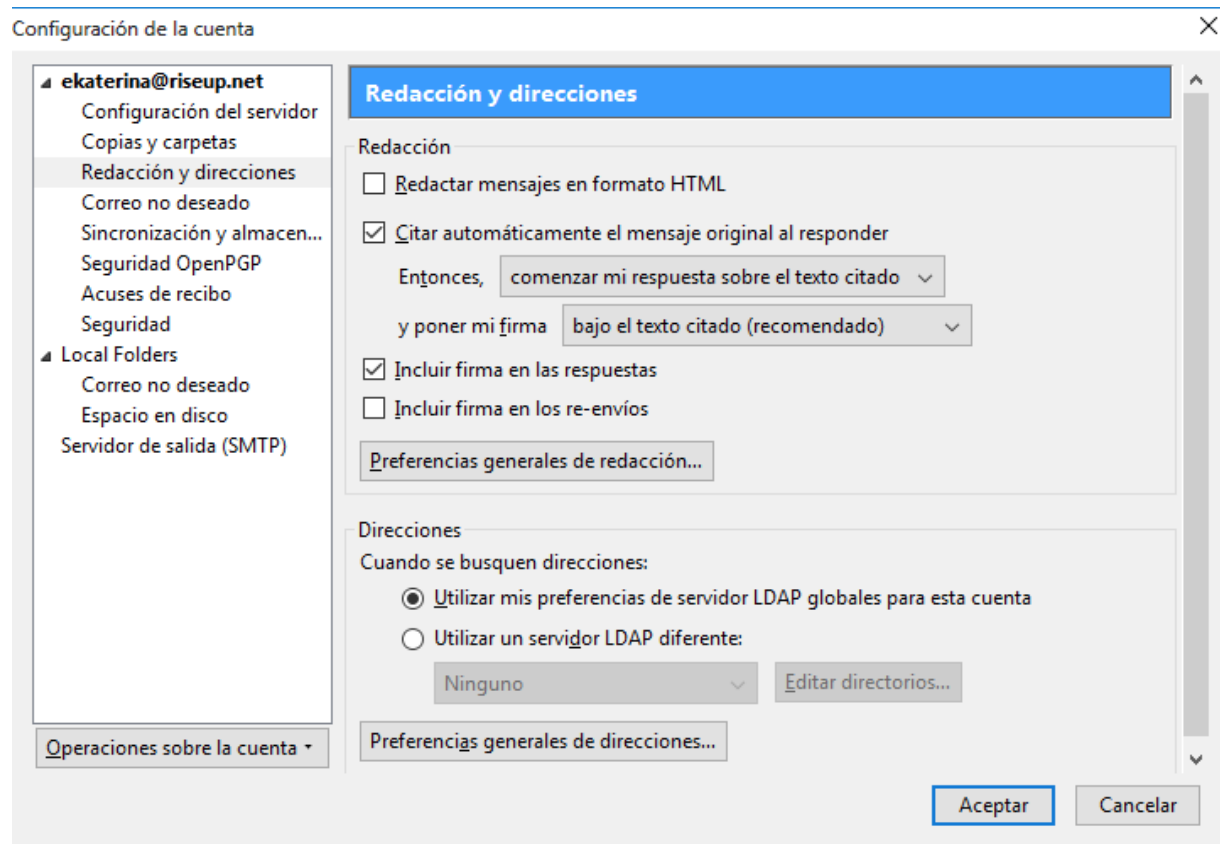


Figura 3: La pantalla de Redacción y Dirección donde el formato Redactar mensajes en HTML no esté marcado

Paso 4. Saca la marca del recuadro [Redactar mensajes en HTML].

Paso 5. Haz clic en [OK].

3.2 CONFIGURAR PREFERENCIAS DE SEGURIDAD DE THUNDERBIRD

Para modificar las preferencias de seguridad de Thunderbird, sigue los pasos a continuación:

Paso 1. Haz clic en  para activar la barra de menú de Thunderbird.

Paso 2. Elige [Opciones > Opciones].

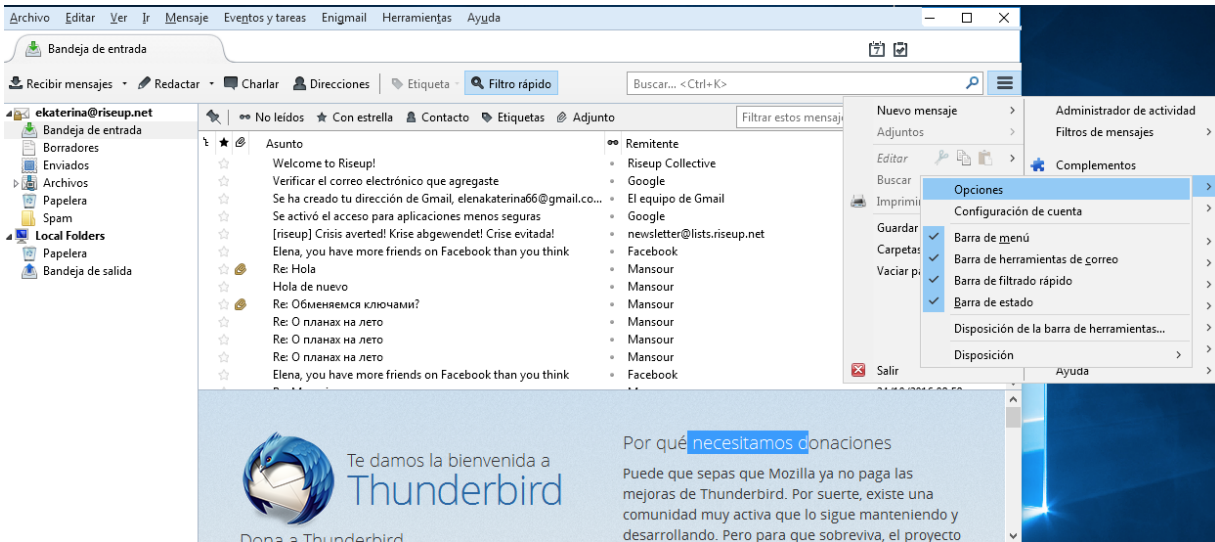


Figura 1: Elegir Opciones a través de la barra de menú de Thunderbird

Paso 3. Haz clic en la pestaña Seguridad.

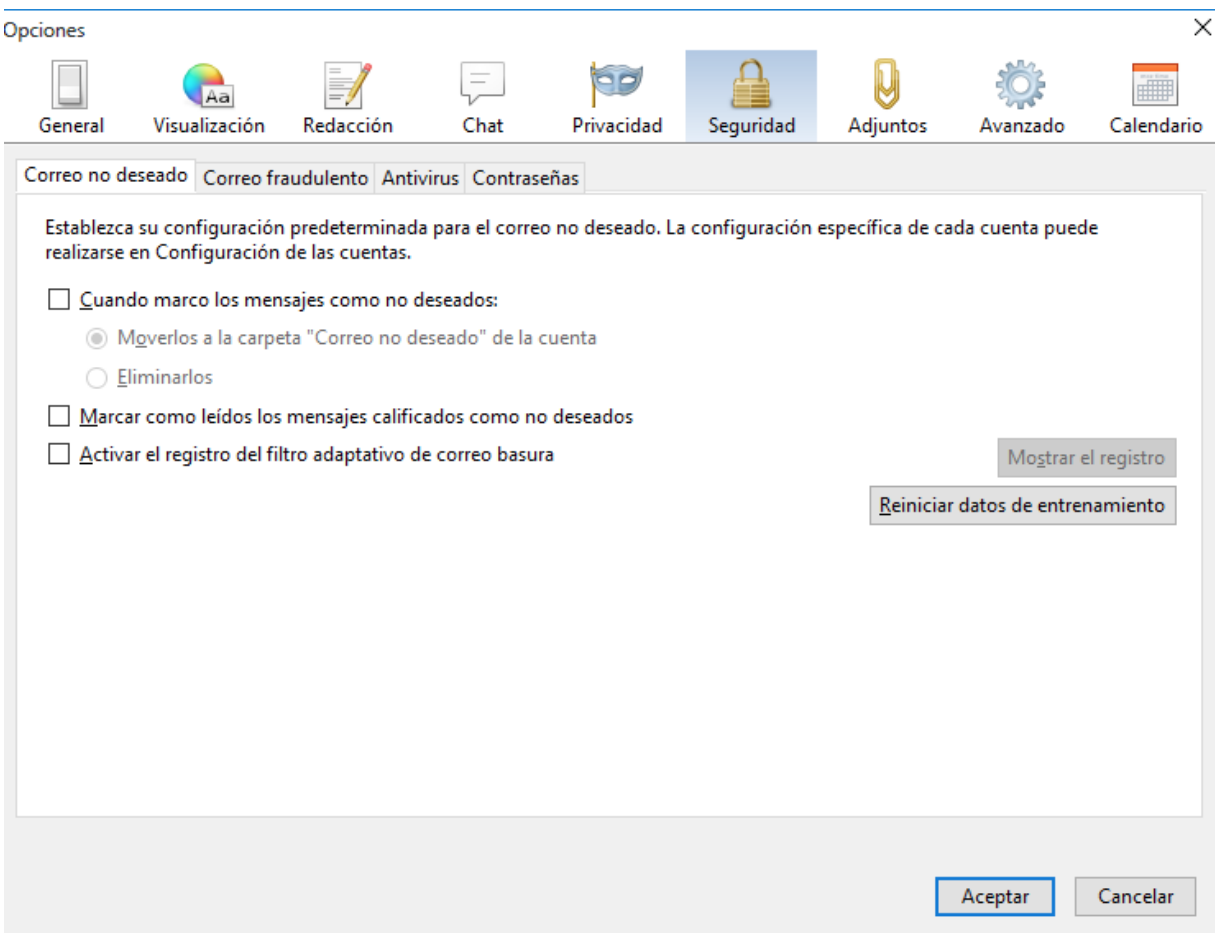


Figura 2: Pantalla de preferencias de seguridad de Thunderbird

Paso 4. Haz clic en la subpestaña *Contraseñas*.

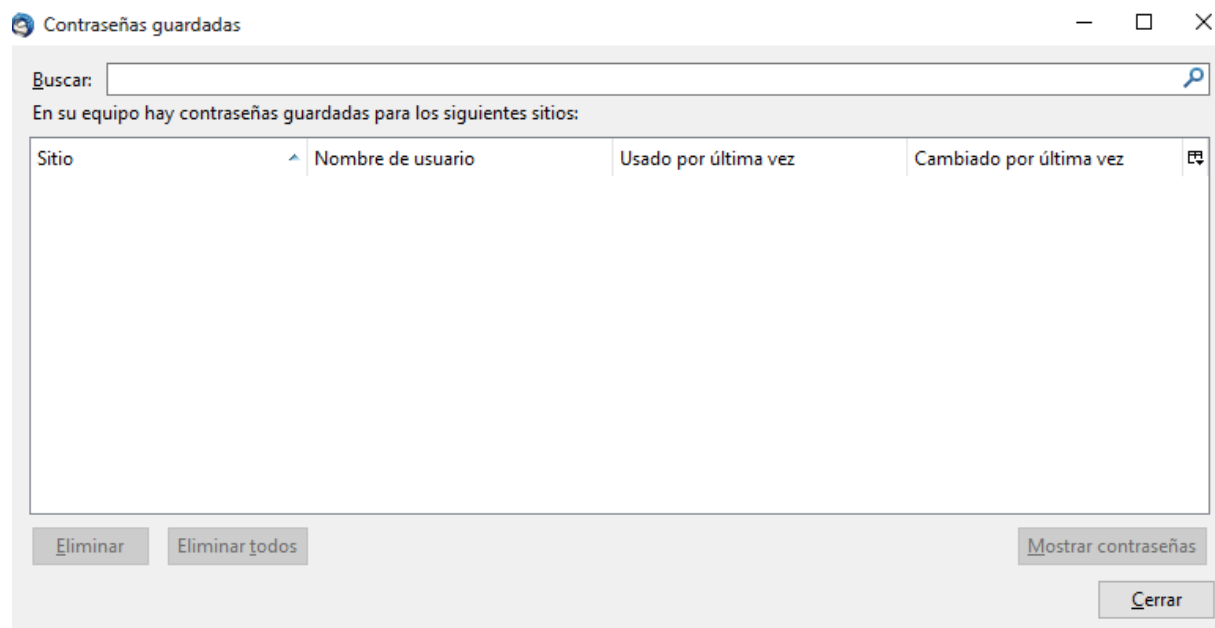


Figura 3: Pestaña de contraseñas

Para ver o eliminar contraseñas de cuentas de correo electrónico guardades en tu computadora, **haz clic** en **[Contraseñas guardadas]**.

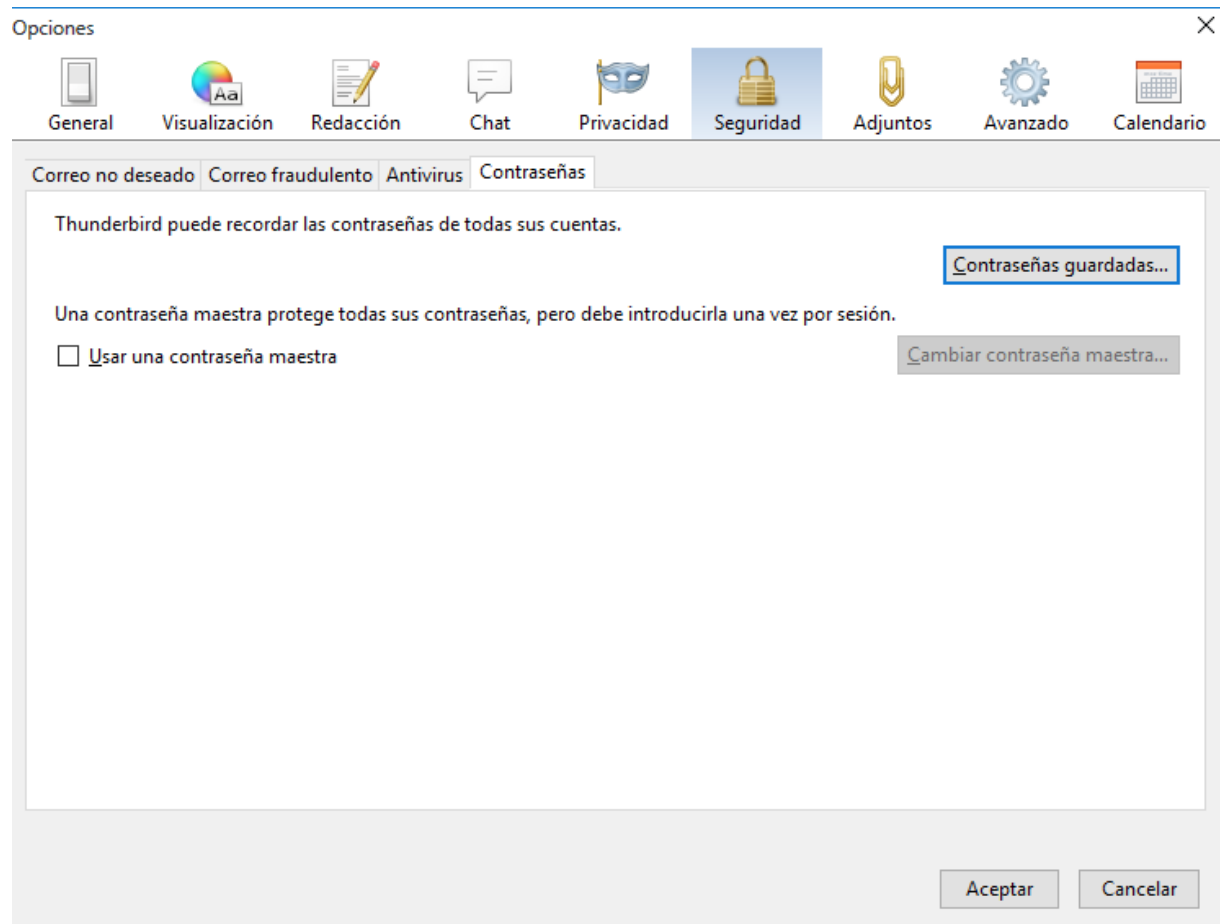


Figura 4: Ventana de contraseñas guardadas

Para eliminar todas las contraseñas guardadas por Thunderbird, **haz clic** en **[Eliminar todo]**. También puedes eliminar contraseñas individuales.

Importante: Recomendamos que protejas tus contraseñas usando una herramienta diseñada específicamente para ese fin. Ver [KeePassX \(../../keepassx/windows\)](https://keepassx.org/..../keepassx/windows) para más información. Sin embargo, si tu intención es permitir que Thunderbird te las recuerde, es extremadamente importante que configures una **contraseña maestra** para que Thunderbird pueda encriptar tus *otras* contraseñas. Es más, aunque *no* quieras que Thunderbird guarde las contraseña de tu cuenta de correo electrónico, tal vez quieras configurar una contraseña maestra. Hacerlo te garantiza que Thunderbird encripte cualquier contraseña que sin querer hayas pedido guardar. Si haces esto, asegúrate de recordar tu contraseña maestra o registrarla en algún lugar seguro (como en una base de datos de [KeePassX](https://keepassx.org/..../keepassx/windows)

(../keepassx/windows)). Y ten en cuenta que Thunderbird te pedirá esa contraseña maestra cada vez que reinicies la aplicación.

Paso 5. Marca el recuadro **[Usar una contraseña maestra]** para activar la siguiente pantalla:

Figura 5: Ventana de Cambiar contraseña maestra

Paso 6. Escribe una contraseña fuerte en ambos campos y haz clic en **[OK]**.

3.3 CONFIGURAR PREFERENCIAS DE PRIVACIDAD DE THUNDERBIRD

Las *cookies* contienen información que los sitios web que visitas envían a tu navegador. Cuando regresas a estos sitios, les envías de vuelta las cookies correspondientes, junto con tu solicitud de contenido. Las cookies se usan por una serie de razones. Por ejemplo, sitios web que te solicitan iniciar sesión a menudo las usan para recordar si ya lo has hecho o no. Pero las cookies también se pueden usar para rastrear tus actividades en línea.

Thunderbird acepta cookies principalmente para operar con fuentes de RSS y grupos de noticias, no para correo electrónico. Recomendamos que inhabilites el respaldo para cookies en Thunderbird. Si esto te impide usar una función de Thunderbird que necesitas, siempre puedes regresar y habilitarlo.

Puedes decirle a Thunderbird que *no* acepte cookies siguiendo los pasos a continuación:

Paso 1. Haz clic en  para activar la barra de menú de Thunderbird.

Paso 2. Elige [Opciones > Opciones].

Paso 3. Haz clic en la pestaña de *Privacidad*.

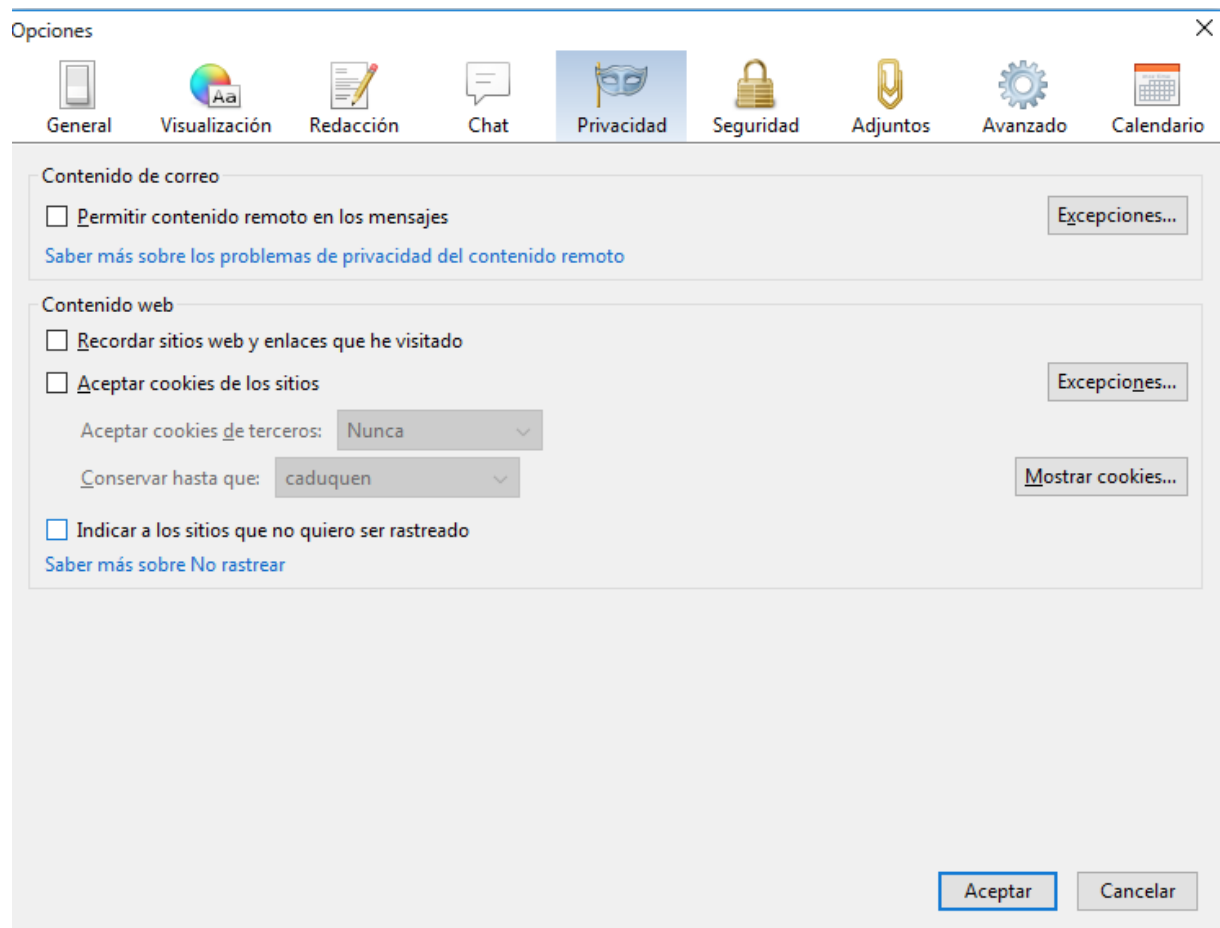


Figura 1: Pestaña de privacidad

Paso 4. Saca la marca de los siguientes recuadros:

- Permitir contenido remoto en los mensajes (todavía puedes habilitar contenido remoto por cada mensaje).
- Recordar los sitios web y enlaces que he visitado.
- Aceptar cookies de los sitios web.

4. ENVIAR Y RECIBIR MENSAJES ENCRIPTADOS

GNU Privacy Guard (GnuPG or GPG) es un software de encriptación libre y de código abierto elaborado por el Proyecto GNU. Cumple con el estándar **OpenPGP** y fue diseñado para interoperar con *Pretty Good Privacy (PGP, o privacidad bastante buena)*, un equivalente comercial elaborado por Phil Zimmermann y está a cargo de *Symantec*.

Enigmail es un complemento de Thunderbird que te permite acceder a las funciones de encriptación de GnuPG desde dentro de Thunderbird.

GnuPG depende de una forma de *criptografía de clave pública* que requiere que cada usuario genere su propio par de *claves*. Este *par de claves* se puede usar para encriptar, desencriptar y firmar contenido digital como mensajes de correo electrónico. Incluye una *clave privada* y una *clave pública*:

- Tu **clave privada** es extremadamente sensible. Cualquiera que haya conseguido una copia de esta clave podrá leer contenido encriptado que estaba dirigido solamente a ti. También podría firmar mensajes para que parezca que *vienen de ti*. Tu *clave privada* está encriptada en sí misma a una contraseña que escogerás cuando generes tu *par de claves*. Debes escoger una contraseña fuerte y cuidar que nadie tenga acceso a tu *clave privada*. Usarás tu *clave privada* para desencriptar mensajes que te envíen quienes tengan una copia de tu *clave pública*.
- Tu **clave pública** está diseñada para que la compartas con otros y no se puede usar para leer un mensaje encriptado ni para falsificar uno firmado. Una vez que tengas una clave pública de corresponsal,

puedes empezar a enviar mensajes encriptados a otra persona. Es la única persona que podrá desencriptar y leer estos mensajes porque nadie más tiene acceso a la *clave privada* que encaja con la *clave pública* que estás usando para encriptarlos. De manera similar, para que alguien *te* envíe correo encriptado, debe obtener una copia de tu *clave pública*. Es importante verificar que la *clave pública* que estás usando para encriptar correo electrónico realmente pertenece a la persona con quien estás tratando de comunicarte. Si tú o tu la persona con quien te comunicas son engañadas para encriptar correo electrónico con la clave pública equivocada, la conversación no será segura.

GnuPG y Enigmail también te permiten adjuntar **firmas digitales** a tus mensajes. Si *firmas* un mensaje usando tu *clave privada*, cualquier destinatario con una copia de tu *clave pública* puede verificar que fue enviada a ti y que su contenido no ha sido adulterado. De manera similar, si tienes una *clave pública* de la persona con quien te comunicas, puedes verificar sus firmas digitales.

4.1 INSTALAR GNUPG Y ENIGMAIL

Esta sección te guiamos para la instalación de **GnuPG** y **Enigmail**.

4.1.1 INSTALAR GNUPG

Para instalar GnuPG, sigue los pasos a continuación:

Paso 1. Navega a la página de descarga de **Gpg4win** en <https://www.gpg4win.org/> (<https://www.gpg4win.org/>).



Figura 1: Sitio web Gpg4win

Paso 2. Haz clic en [Descargar Gpg4win].

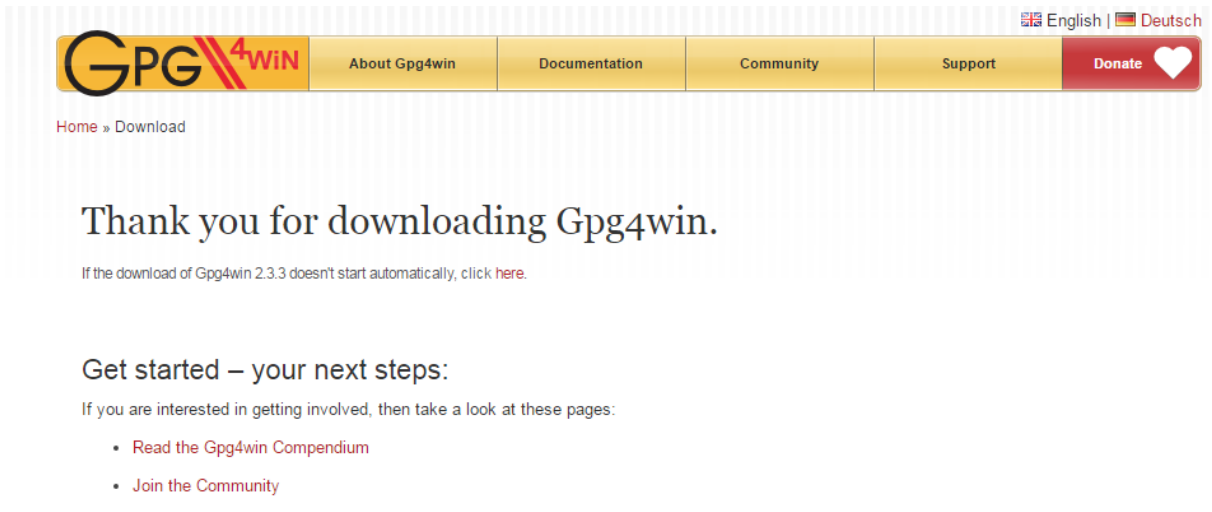


Figura 2: Página de descarga de Gpg4win

Paso 3. Haz clic en [Gpg4win 2.3.1] o cualquier otra publicación más reciente.

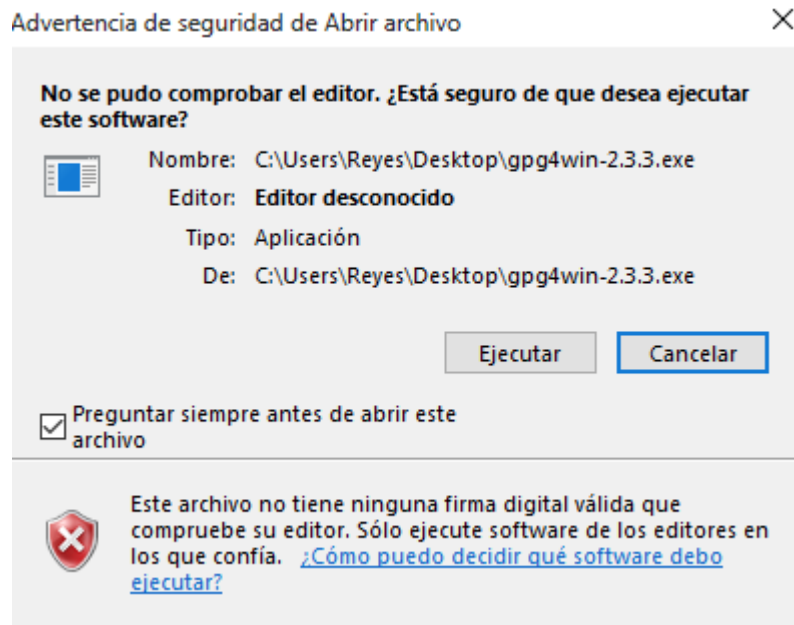


Figura 3: Descargar Gpg4win

Paso 4. Haz clic en [Guardar archivo] para descargar Gpg4win.

Paso 5. Haz clic derecho en el archivo descargado de gpg4win y **elige [Abrir]**.

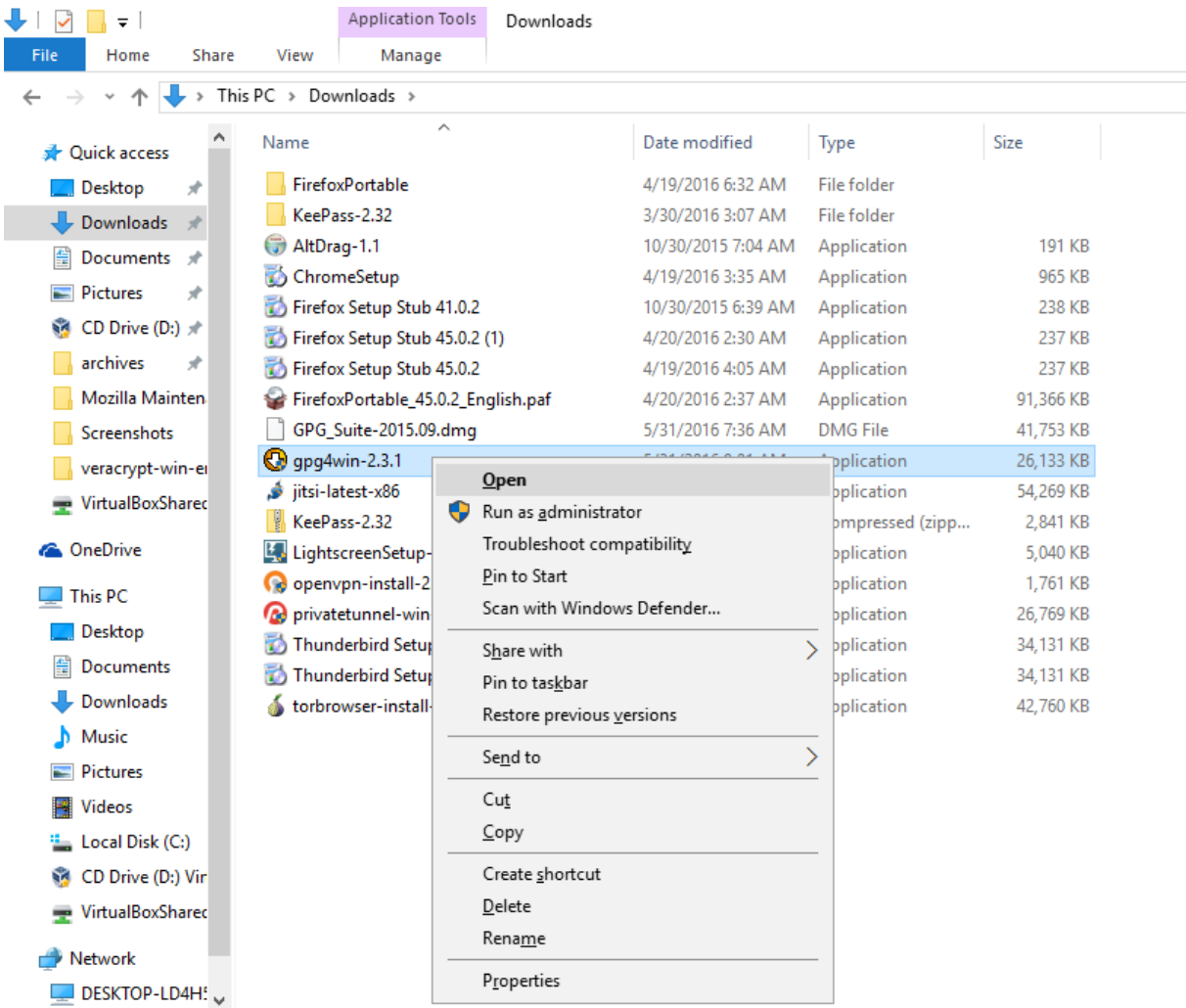


Figura 4: Abrir el archivo gpg4win

Paso 6. Elige un idioma para la configuración de Gpg4win.

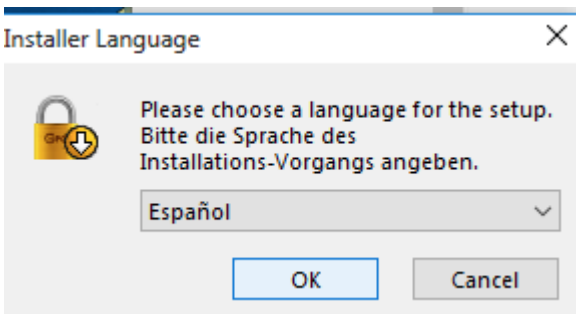


Figura 5: idioma del instalador

Paso 7. Haz clic en [Siguiente] para empezar el proceso de instalación de

Gpg4win.



Figura 6: Ventana de configuración Gpg4win

Paso 8. Lee el Acuerdo de licencia y **haz clic** en **[Siguiente]**.

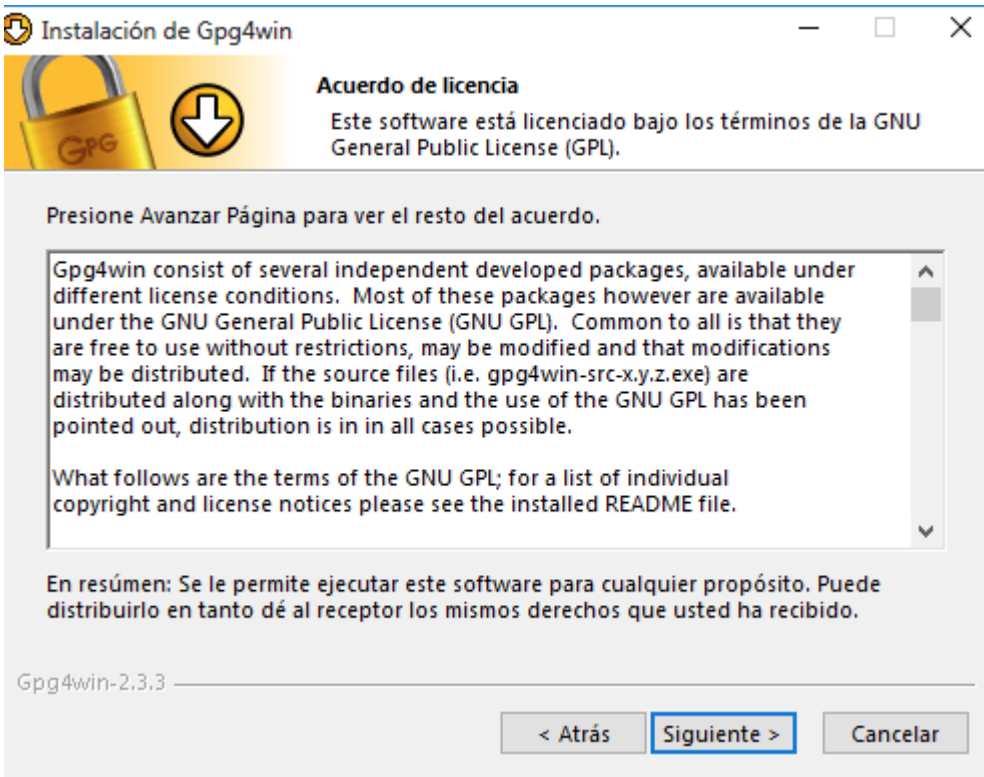


Figura 7: Acuerdo de licencia de Gpg4win

Paso 9. Elige qué funciones de Gpg4win quieres instalar. Las opciones por defecto están bien.

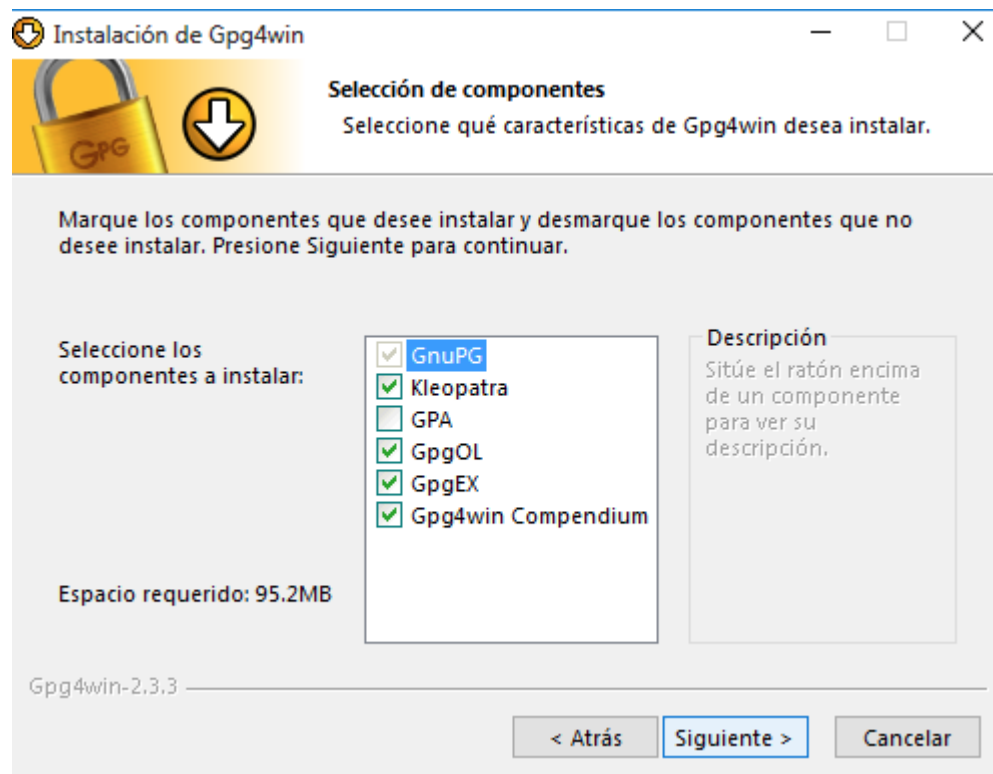


Figura 8: Funciones de Gpg4win

Paso 10. Elige la ubicación donde quieres instalar Gpg4win y **elige [Siguiente]**.

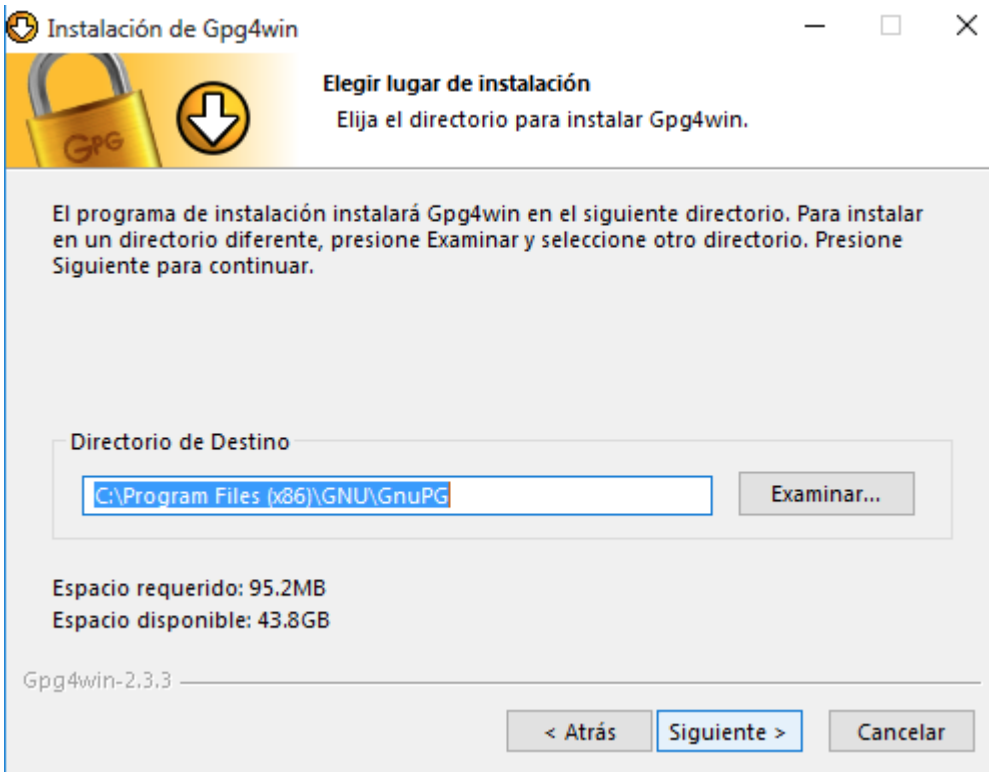


Figura 9: Ubicación de instalación de Gpg4win

Paso 11. Elige [Siguiete].

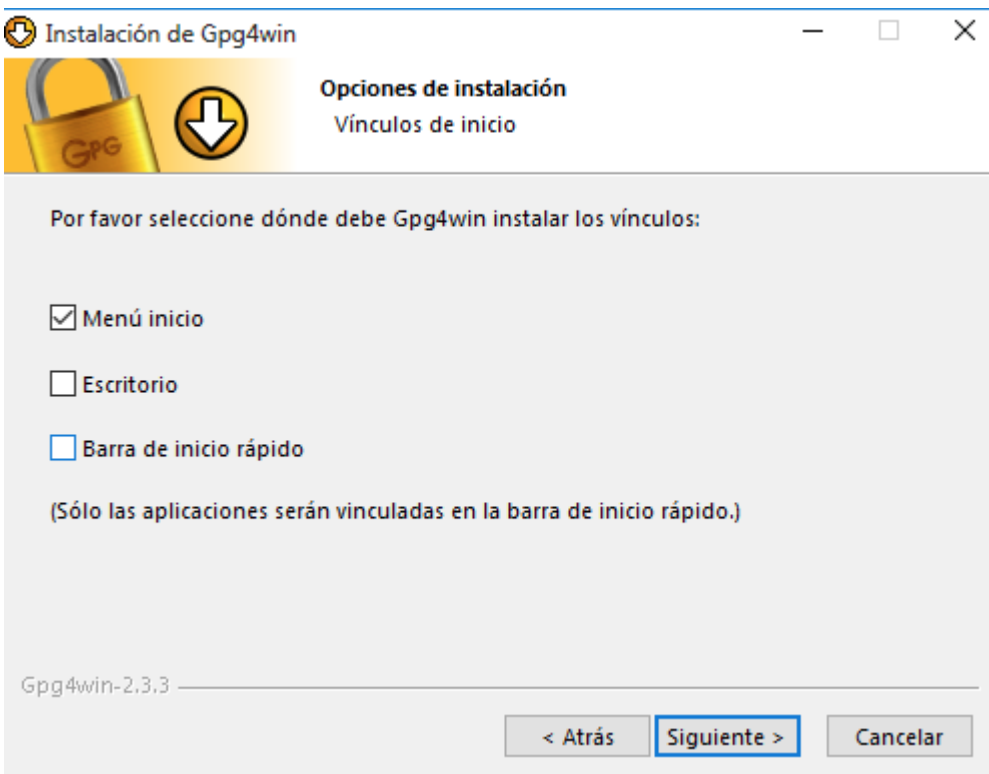


Figura 10: Opciones de instalación de Gpg4win

Paso 12. Escoge una carpeta de menú de inicio para los accesos directos de Gpg4win, **haz clic** en **[Siguiente]** para empezar a instalar Gpg4win.

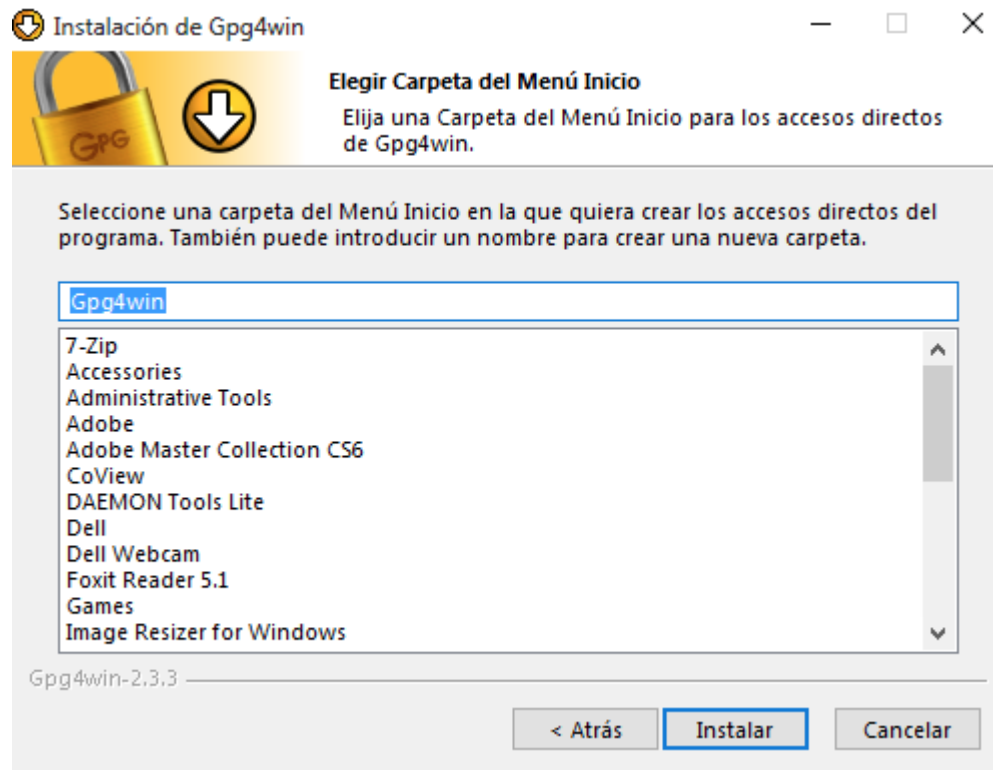


Figura 11: Elegir accesos directos de Gpg4win

Paso 13. Haz clic en **[Siguiente]** para empezar a instalar Gpg4win.

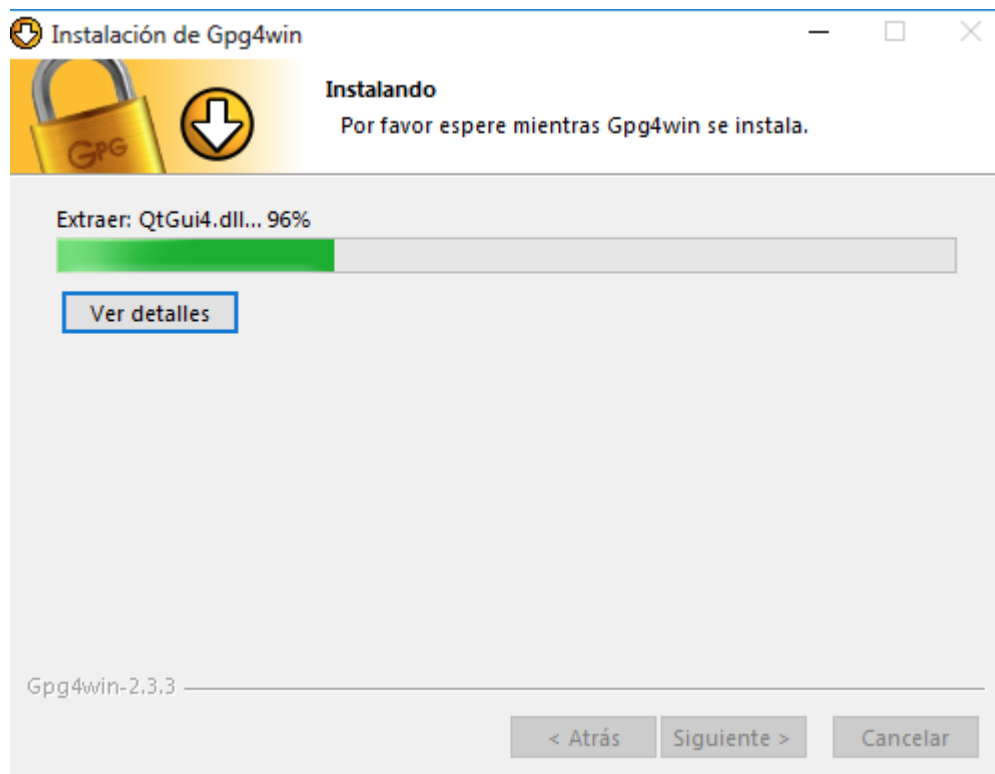


Figura 12: Instalar Gpg4win

Paso 14. Haz clic en [Siguiete].

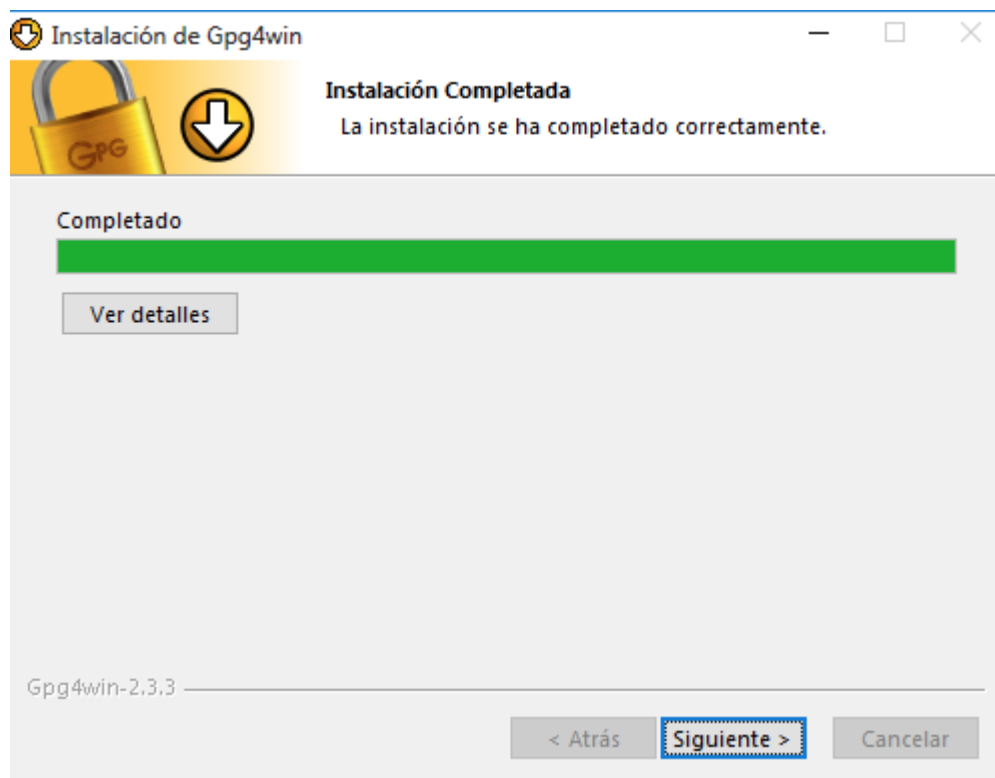


Figura 13: Proseguir con el proceso de instalación de Gpg4win

Paso 15. Haz clic en [Terminar] para completar el proceso de instalación de Gpg4win.



Figura 14: Completar el proceso de instalación de Gpg4win

4.1.2 INSTALAR ENIGMAIL

Para instalar **Enigmail**, sigue los pasos a continuación.

Paso 1. Inicia Thunderbird e inicia sesión en tu cuenta.



Figura 1: Thunderbird

Paso 2. Haz clic en * .

Figura 2: Abrir el administrador de complementos

Paso 3. Elige [Complementos] para abrir el *Administrador de complementos*.

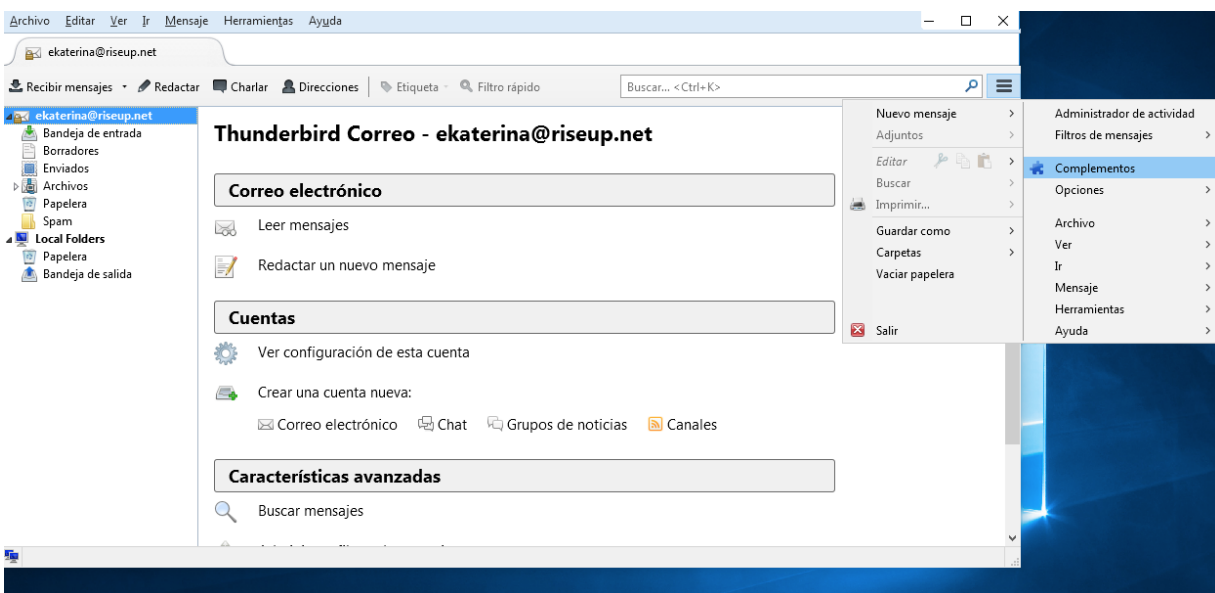


Figura 2: Abrir el Administrador de complementos

Paso 4. Escribe [Enigmail] en el campo de búsqueda en la esquina superior derecha del *Administrador de complementos* y presiona **Aceptar.**

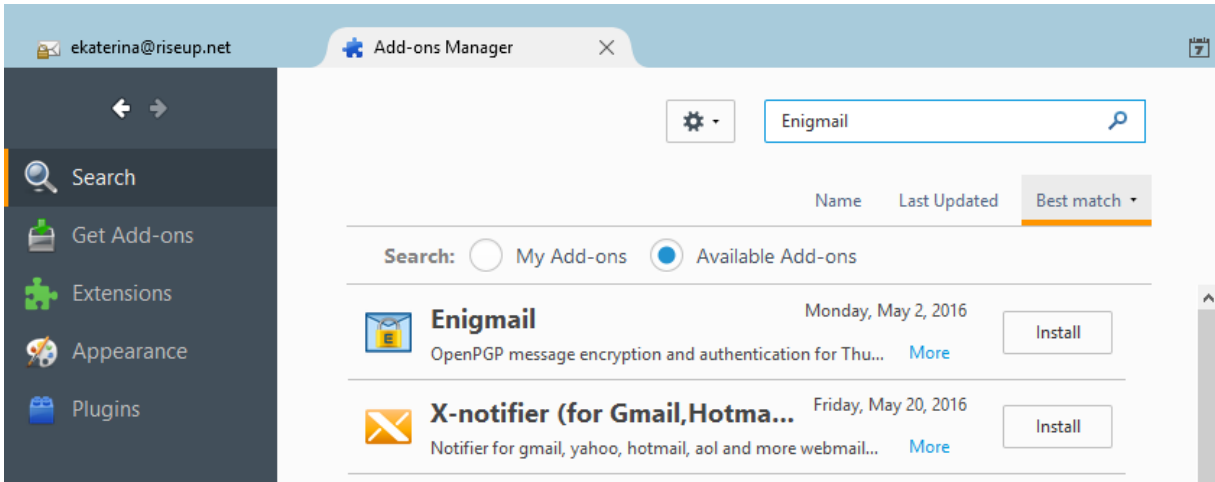


Figura 3: Encontrar el complemento de Enigmail

Paso 5. Haz clic en [Instalar] al lado de la línea de **Enigmail para empezar a instalar el complemento.**

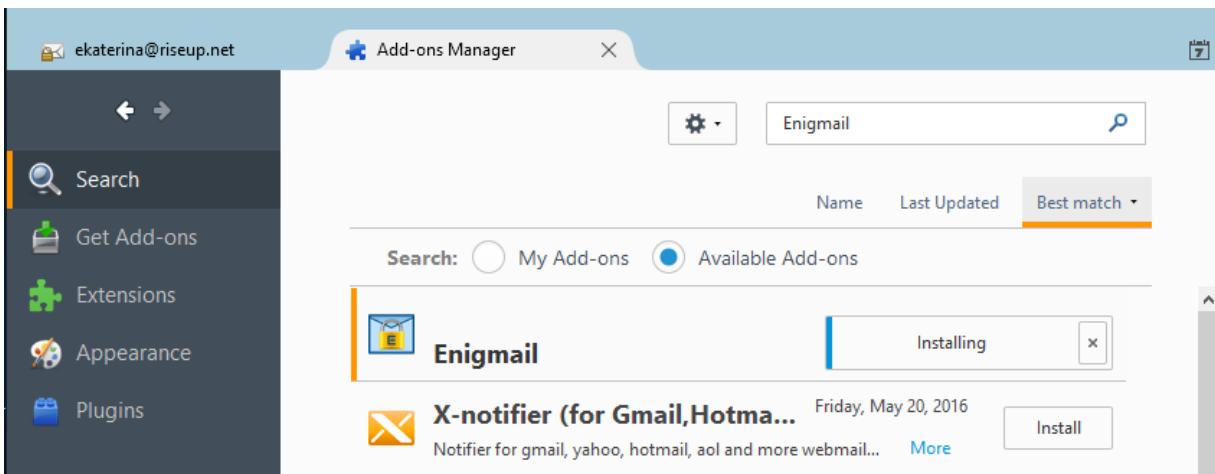


Figura 4: Instalar Enigmail

Cuando Thunderbird haya terminado de instalar el complemento, te lo dirá.

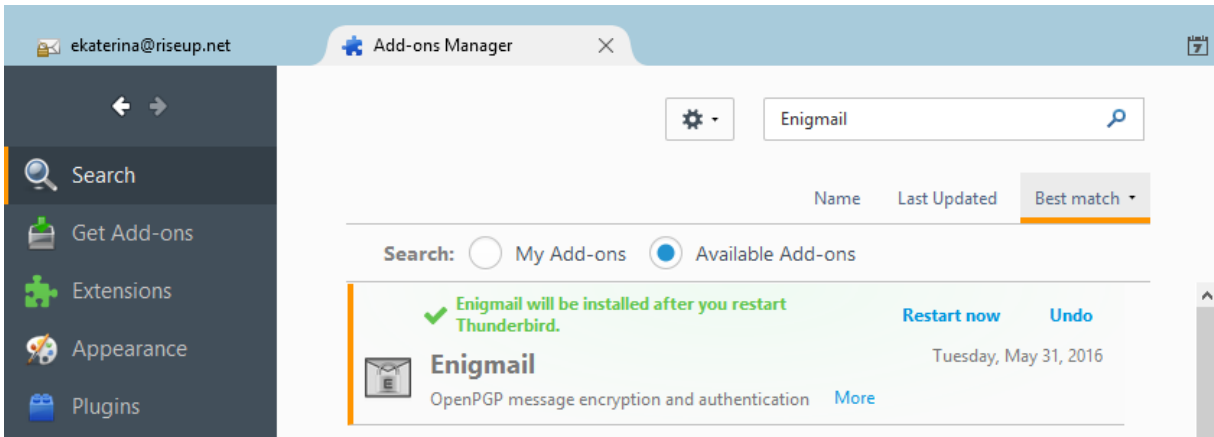


Figura 5: Enigmail instalado

Paso 6. Haz clic en [Reiniciar ahora] para reiniciar Thunderbird y completar la instalación de Enigmail.

Cuando **Thunderbird** se reinicie, se abrirá automáticamente el *Asistente de configuración* de Enigmail, a través del cual puedes generar claves de encriptación.

4.2 GENERAR CLAVES DE ENCRIPCIÓN Y CONFIGURAR ENIGMAIL

Esta sección la generación de un *par de claves* de **GnuPG** y la configuración de **Enigmail**.

4.2.1 GENERAR CLAVES DE ENCRIPCIÓN

Para generar un *par de claves* de **GnuPG**, sigue los pasos a continuación.

Paso 1. Haz clic en  y elige [Enigmail > Asistente de configuración]. Esto abrirá el Asistente de configuración de GnuPG.

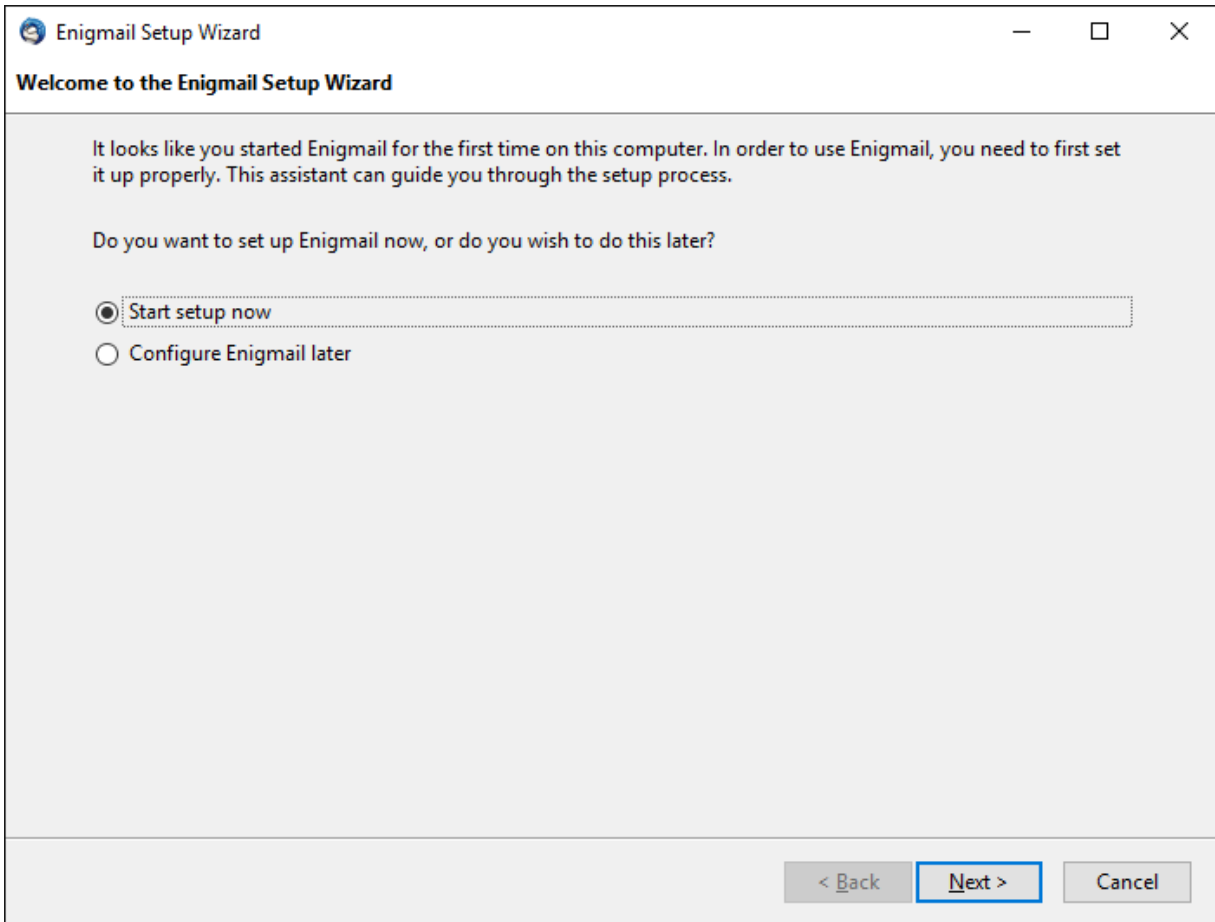


Figura 1: Asistente de configuración de Enigmail

Paso 2. Elige [Iniciar configuración ahora] y haz clic en [Siguiente].

Paso 3. Elige [Prefiero una configuración estándar (recomendado para principiantes)] y haz clic en [Siguiente].

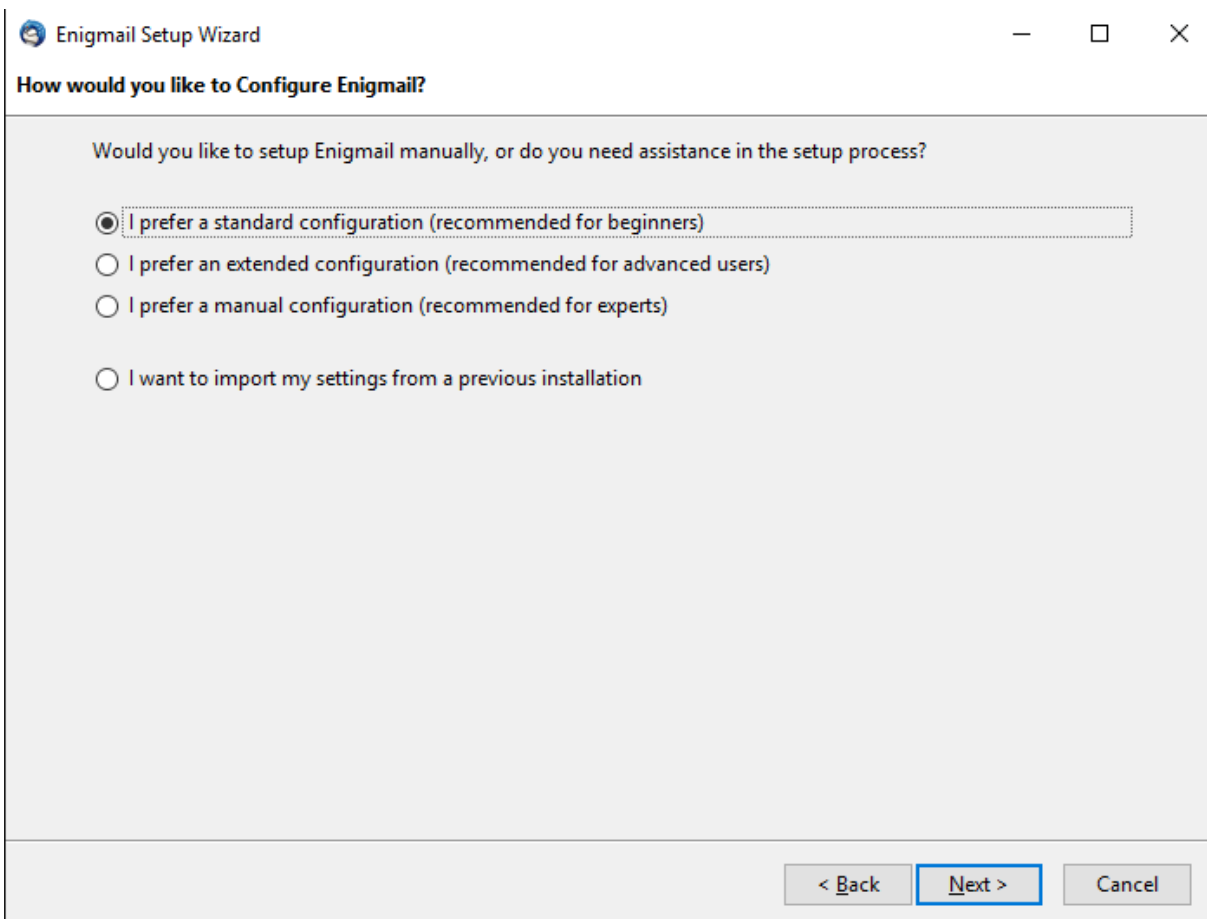


Figura 2: Configurar Enigmail

Paso 4. Escoge una contraseña fuerte y **escríbela** en ios dos campos que muestran la siguiente pantalla:

Enigmail Setup Wizard

Create Key
Create a new Key Pair

This dialog will create a pair of two keys:
Your **public key** is **for others** to send you encrypted emails. You can distribute it to everybody.
Your **private key** is **for yourself** to decrypt these emails and to send signed emails. You should give it to nobody.

Your **passphrase** is a password to protect your private key. It prevents misuse of your private key. The passphrase should be a phrase containing at least 8 characters, digits and punctuation marks. Umlauts (e.g. ä, é, ñ) and language-specific characters are **not** recommended.

Account / User ID:
Elena Katerina <ekaterina@riseup.net> - ekaterina@riseup.net

Passphrase

Please confirm your passphrase by typing it again

Passphrase quality:

< Back Next > Cancel

Figura 3: Elegir una contraseña para tu par de claves de GnuPG

Nota: Esta contraseña se usará para encriptar tu clave privada, que es lo que te permite firmar los correos electrónicos que envías y desencriptar los correos electrónicos que recibes. No debes compartirla con nadie. Por eso, es importante que escojas una contraseña fuerte y que no la olvides. Puedes leer en más en la guía **Crear y conservar contraseñas fuertes** ([../passwords](#)).

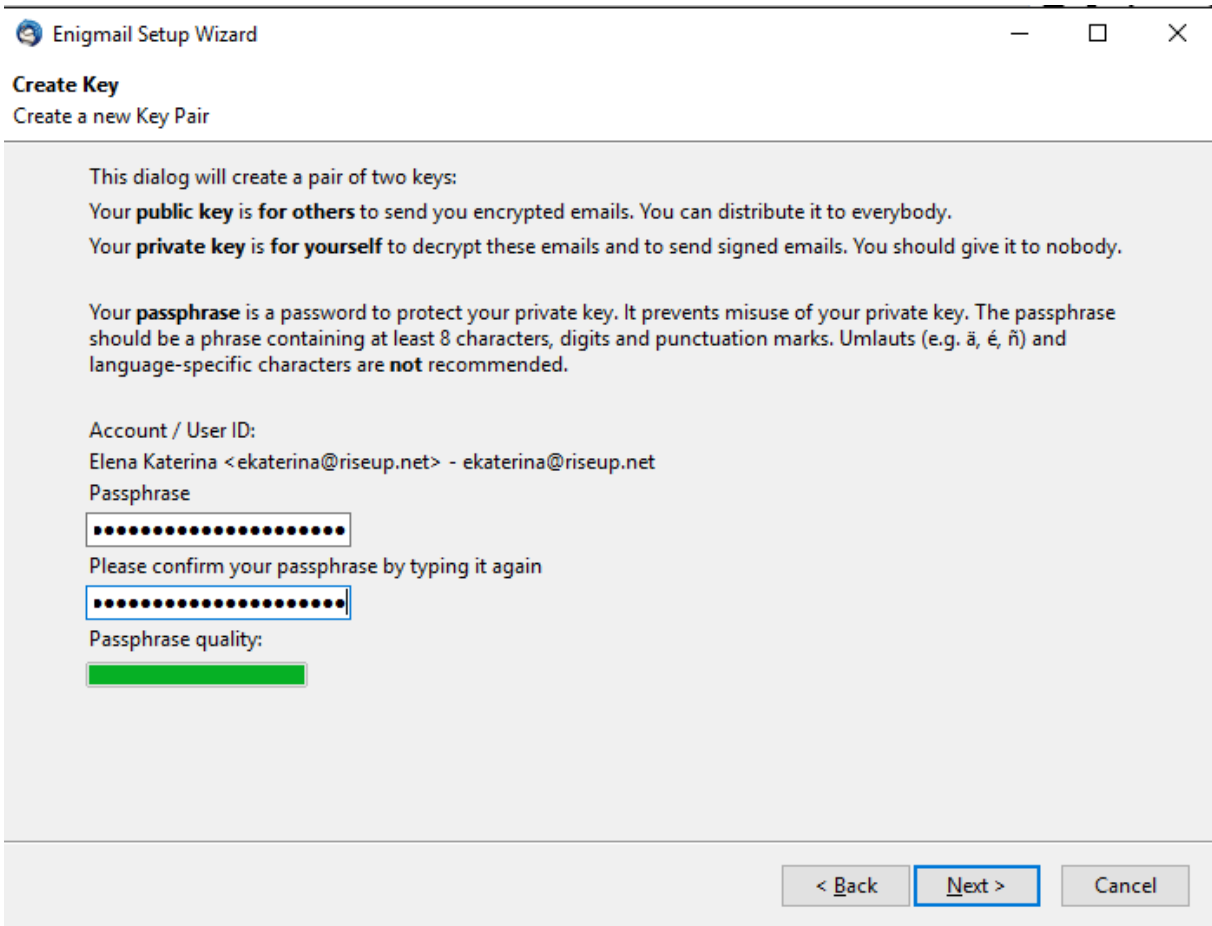


Figura 4: Escribir una contraseña para tu par de claves de GnuPG

Paso 5. Haz clic en [Siguiente] para generar una par de claves de encriptación.

Espera hasta que la generación de la clave se haya completado.

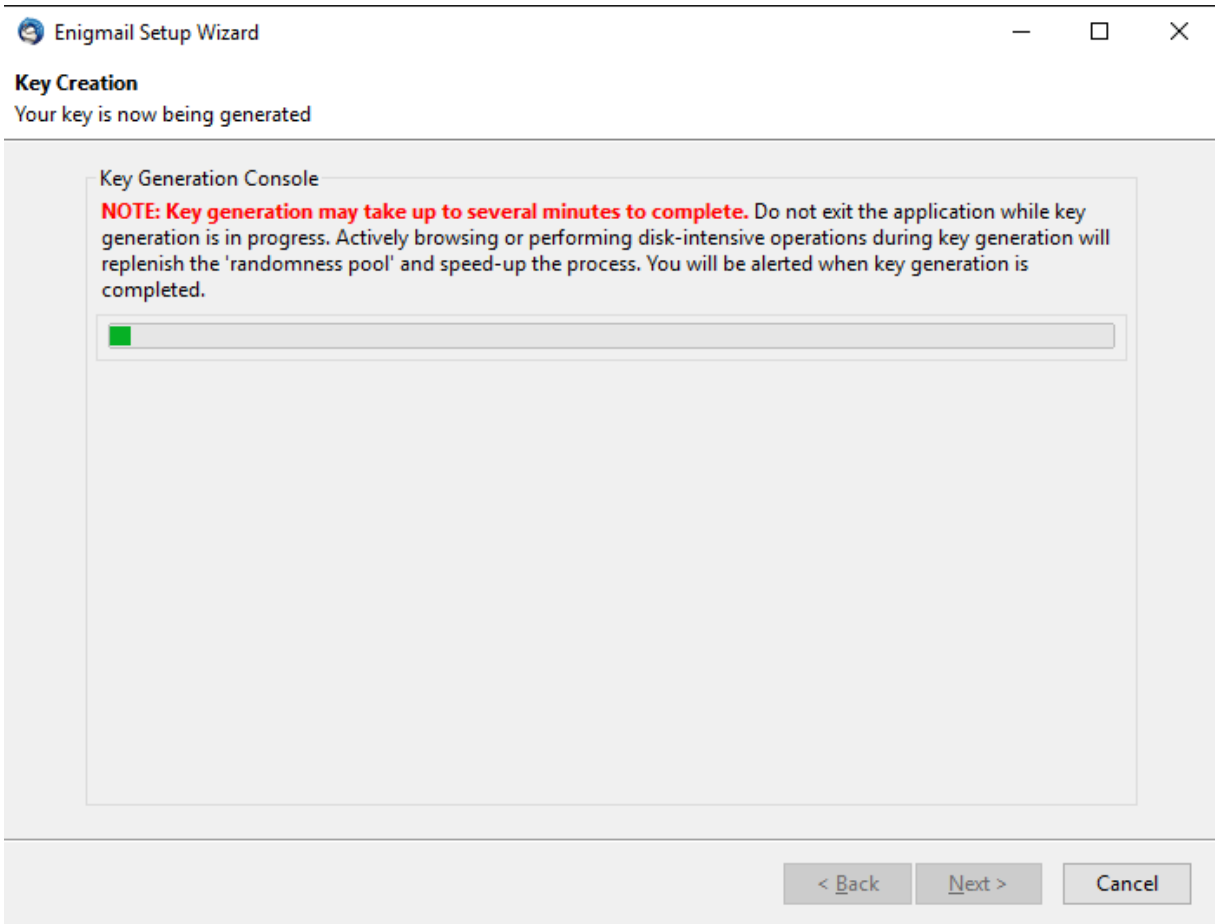


Figura 5: Creación de clave

Cuando Enigmail haya terminado de generar tu *par de claves* de GnuPG, te lo dirá, y aparecerá un botón de *Generar un certificado de revocación*.

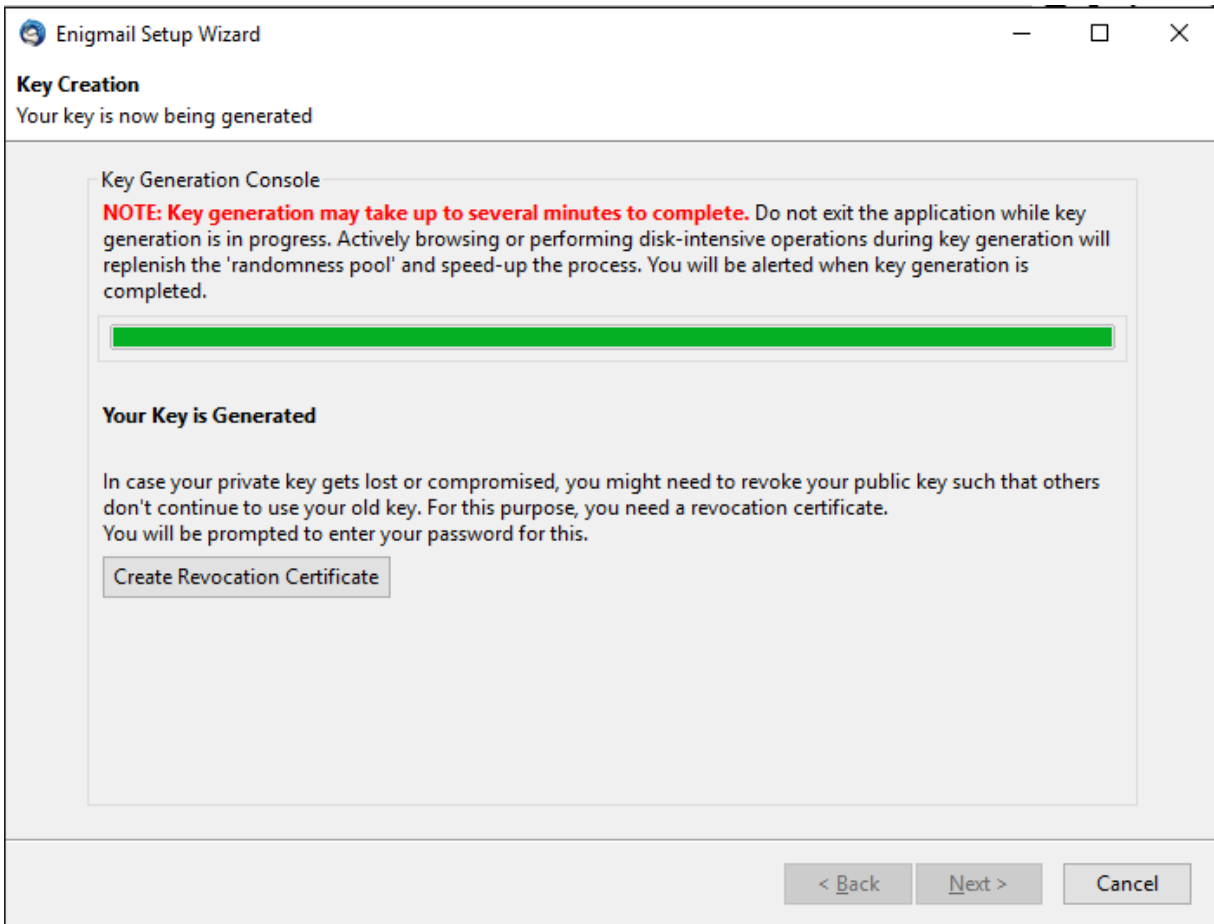


Figura 6: Enigmail listo para generar un certificado de revocación

Debes generar un *certificado de revocación* para que puedas dar a conocer a otros cuando una clave en particular ya no sea válida. Eso puede pasar si:

- Dejas de usar un par de claves
- Pierdes una clave privada
- Olvidas la contraseña de una clave privada
- Sospechas que una clave privada ha dejado de ser segura o si se ha compartido con otros

Es particularmente importante que generes un certificado de revocación si piensas cargar tu clave pública a un servidor de claves. No hay otra manera de "borrar" una clave una vez que la hayas cargado, y no es conveniente tener claves que hayan dejado de ser seguras dando

vueltas en un servidor de claves generando confusión entre las personas.

Paso 6. Haz clic en [Crear Certificado de Revocación].

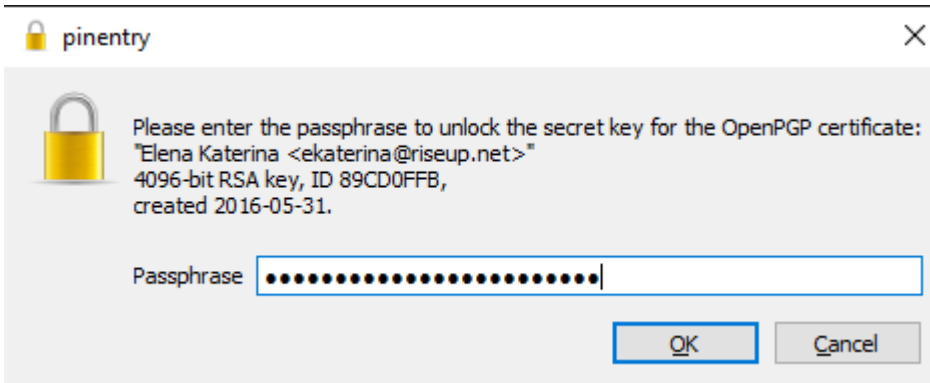


Figura 7: Enigmail pide tus contraseñas para inicio de sesión

Paso 7. Escribe la contraseña que escogiste el crear tu *par de claves* de **GnuPG**.

Paso 8. Escoge un nombre y ubicación para el archivo de tu *certificado de revocación*.

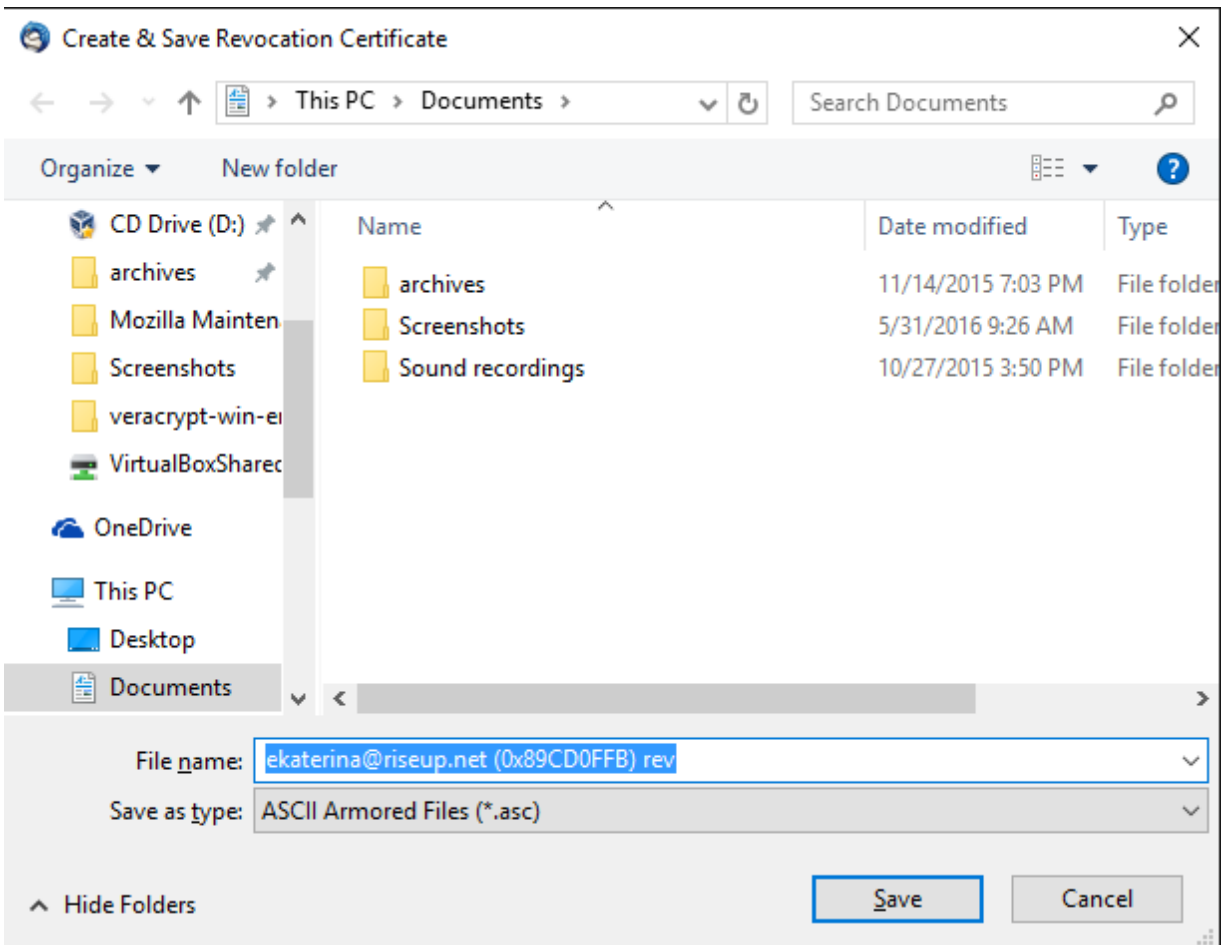


Figura 8: Elegir un nombre y ubicación para el archivo de tu certificado de revocación

En este ejemplo, podremos el *certificado de revocación* en la carpeta *Documentos*, pero puedes guardarlo en cualquier lugar seguro.

Paso 9. Haz clic en [Guardar] para mostrar la advertencia de *Enigmail* sobre la importancia de mantener seguro tu *certificado de revocación*.

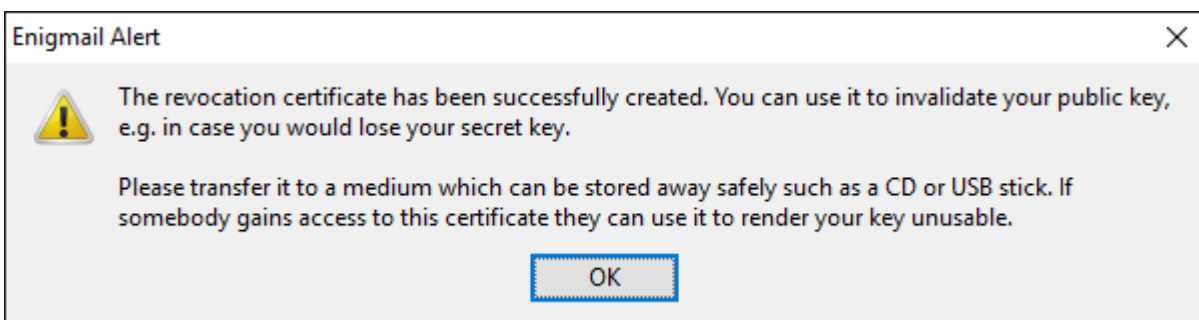


Figura 9: Advertencia del Certificado de revocación

Paso 10. Haz clic en [OK] para regresar al Asistente de configuración.

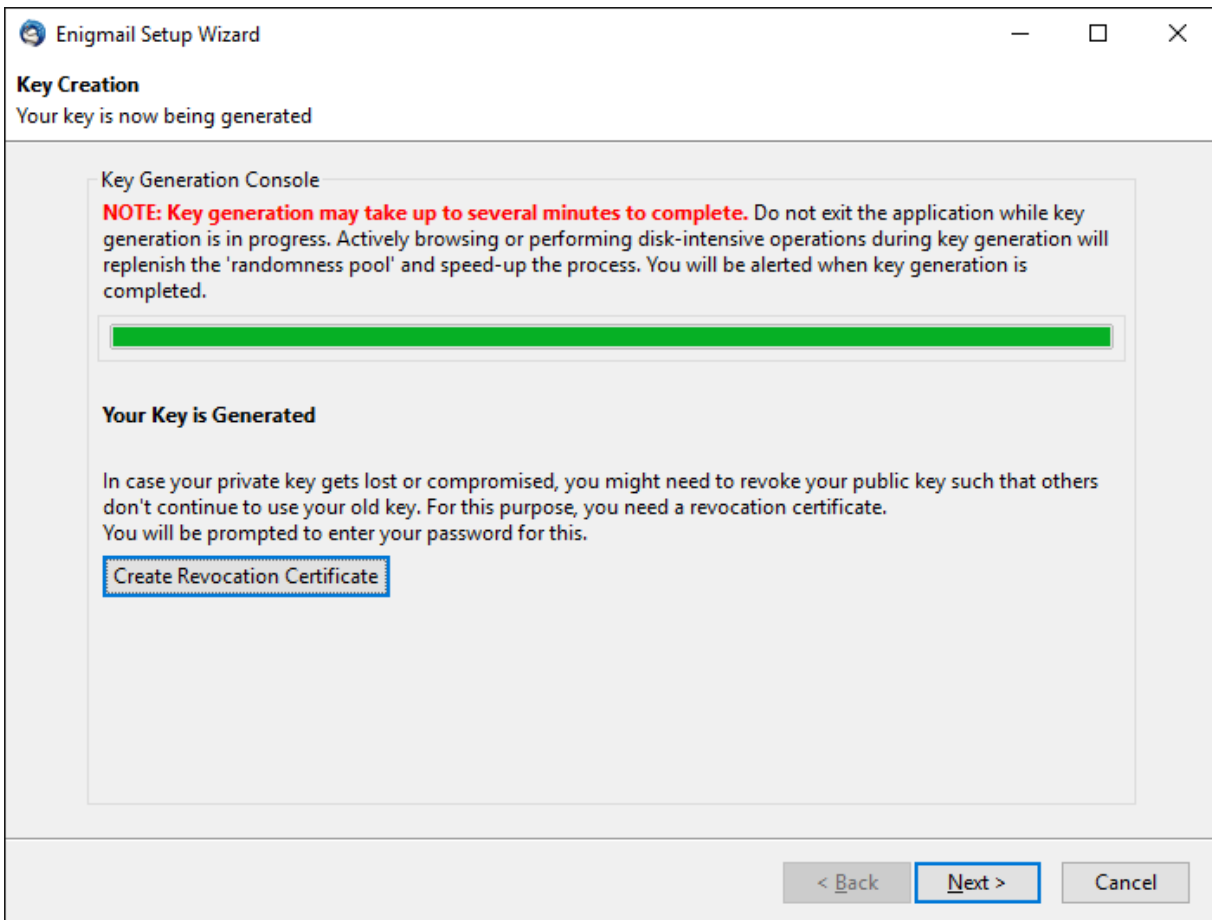


Figura 10: Asistente de configuración de Enigmail

Paso 11. Haz clic en [Siguiente] para completar el proceso de generación de clave.

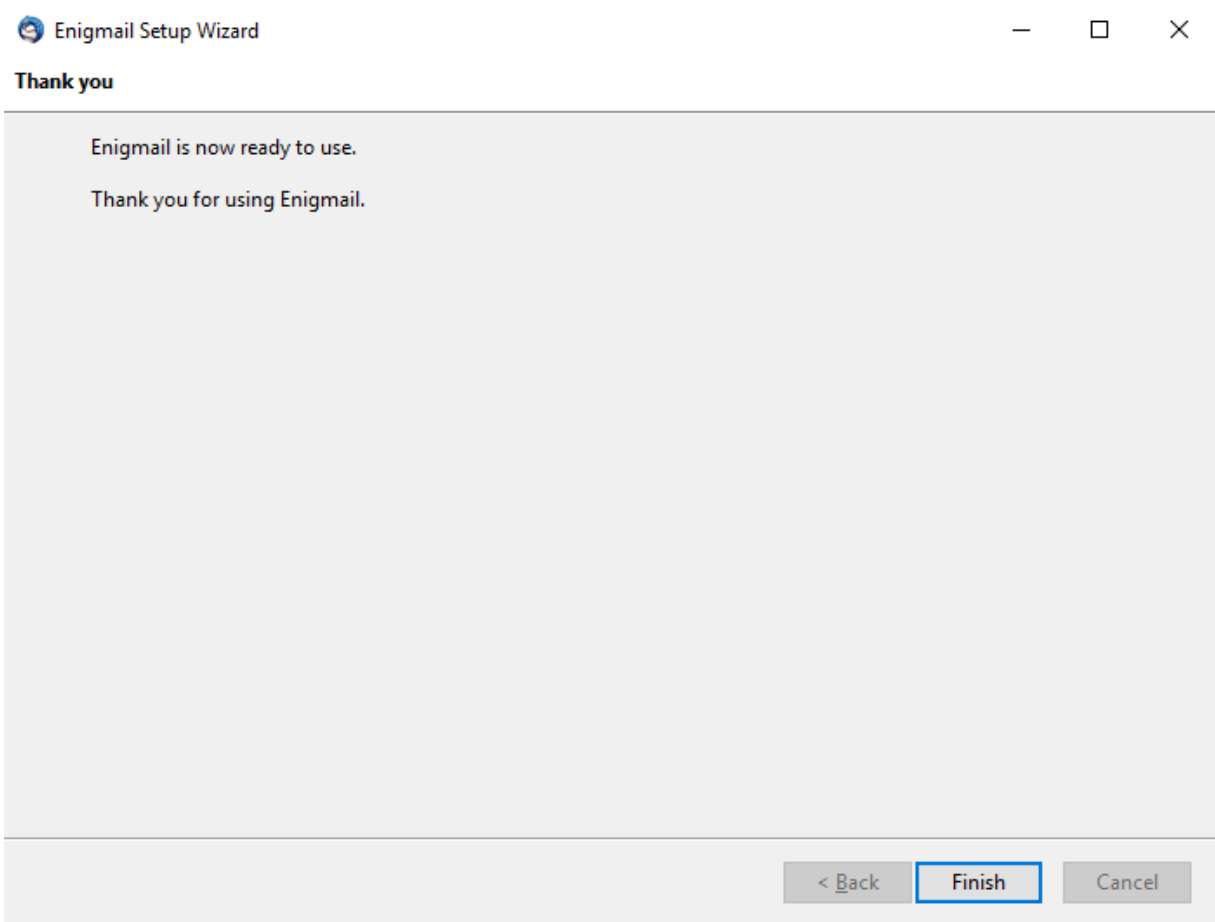


Figura 11: Pantalla de Gracias de Enigmail

Paso 12. Haz clic en **[Terminar]** para salir del *Asistente de configuración* y regresar a Thunderbird.

4.2.2 CONFIGURAR ENIGMAIL PARA QUE FUNCIONE CON TU CUENTA DE CORREO ELECTRÓNICO

Debes habilitar Enigmail para cada cuenta de correo electrónico en Thunderbird, a través de la cual quieras enviar y recibir correo electrónico encriptado **GnuPG**. Para hacerlo, sigue los pasos a continuación.

Paso 1. Haz clic en  y elige **[Opciones > Configuraciones de cuenta]**.

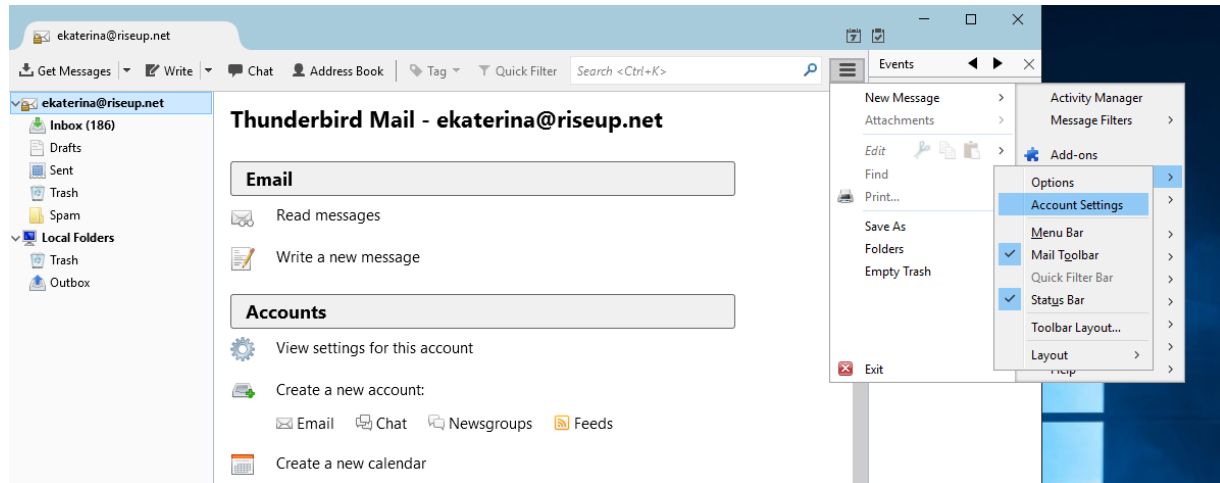


Figura 1: Abrir Configuraciones de cuenta de Thunderbird

Esto abrirá la pantalla de *Configuraciones de cuenta*.

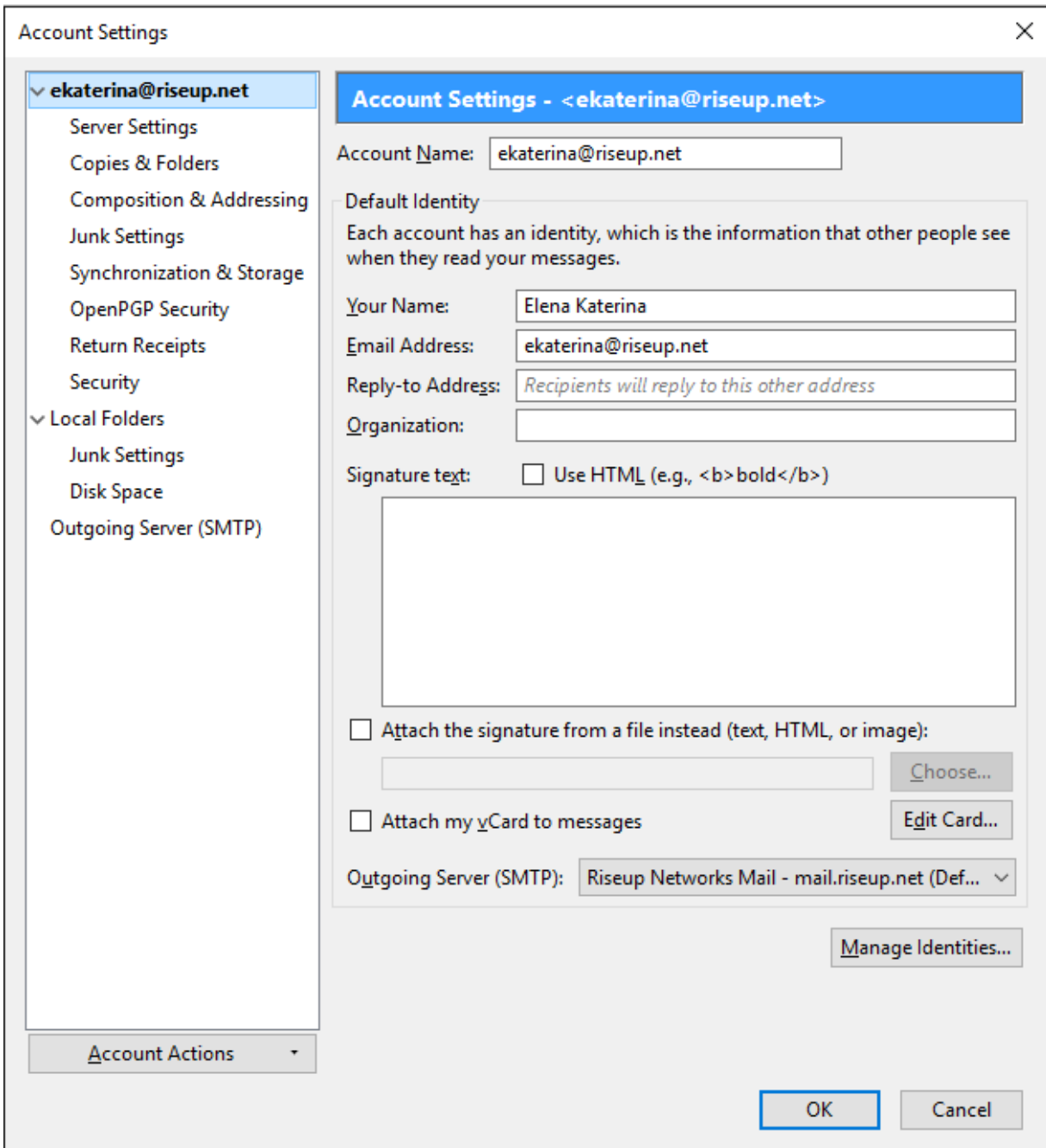


Figura 2: Pantalla de configuraciones de cuenta de Thunderbird

Paso 2. Haz clic en **[OpenPGP Security]** debajo de la cuenta con la que quieres enviar y recibir correo electrónico encriptado.

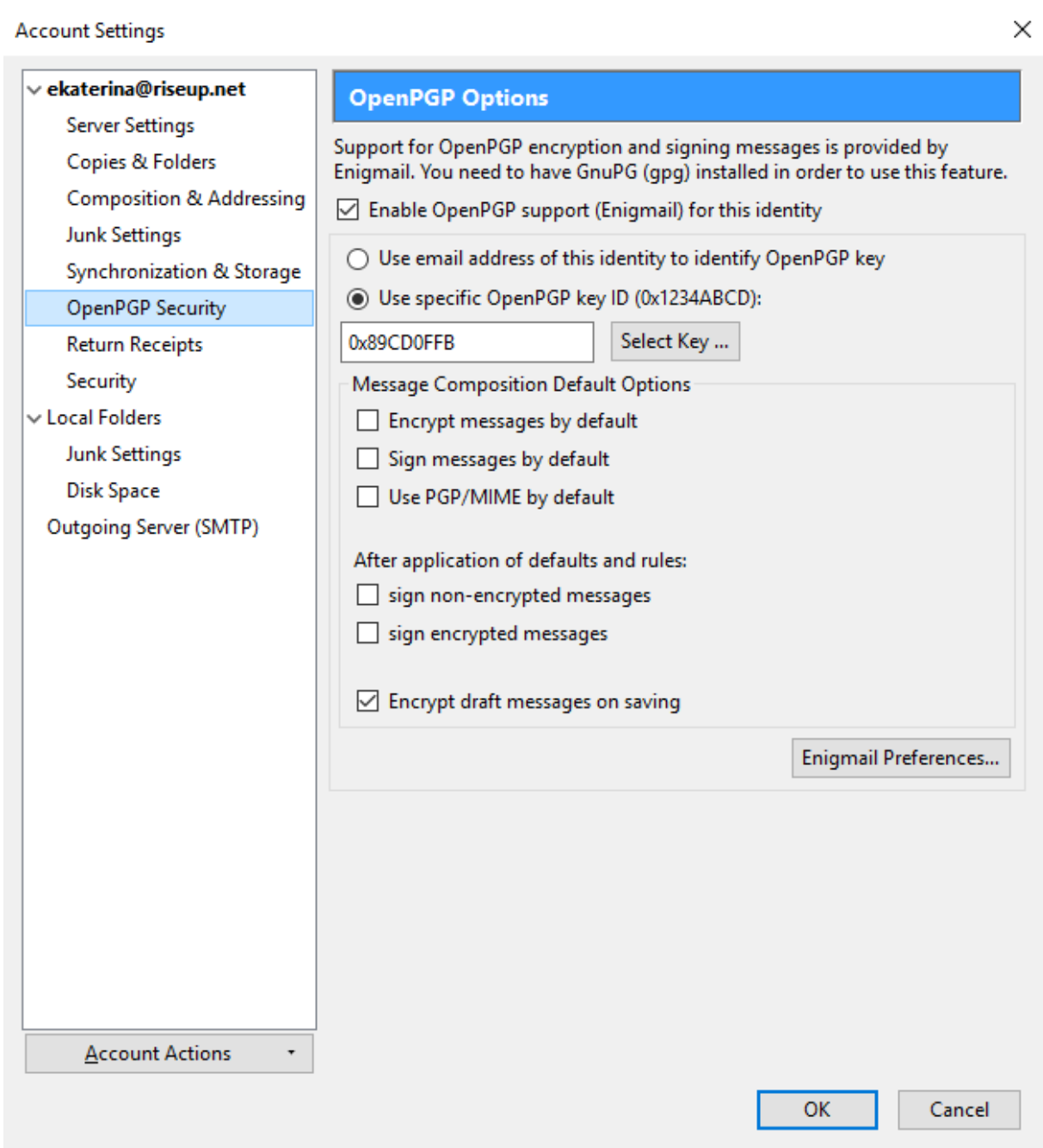


Figura 3: Configuraciones OpenPGP de Enigmail para una cuenta de correo electrónico en Thunderbird

Esta pantalla te permite configurar diversas preferencias de **Enigmail** relacionadas con la encriptación de correo electrónico. Si has generado tu *par de claves* de **GnuPG** siguiendo las instrucciones de la sección anterior – antes de agregar una sola cuenta a **Thunderbird** – esta cuenta ya debería estar configurada para funcionar con **Enigmail**. También debe estar

enlazada con el *par de claves* que generaste. Si no es así, sigue con el *Paso 3*, de abajo. Si es así, puedes saltarte hasta la *Figura 6*.

Paso 3. Marca el recuadro al lado de **[Habilitar OpenPGP para que opere con (Enigmail) para esta identidad]**.

Paso 4. Haz clic en **[Elegir clave...]** para abrir la ventana de *Elige clave OpenPGP para encriptación*.

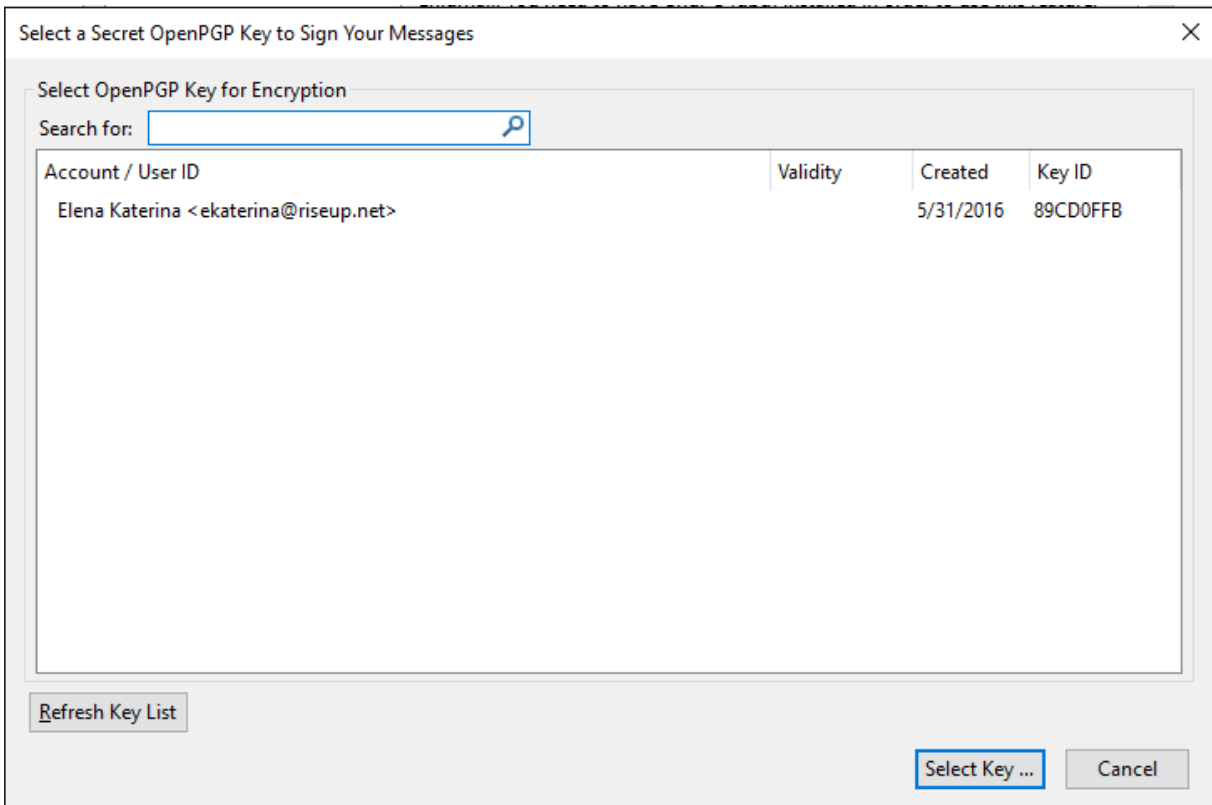


Figura 4: Pantalla de Enigmail de Elegir clave de OpenPGP para encriptación

Paso 5. Elige el *par de claves* que quieres usar para esta cuenta de correo electrónico.

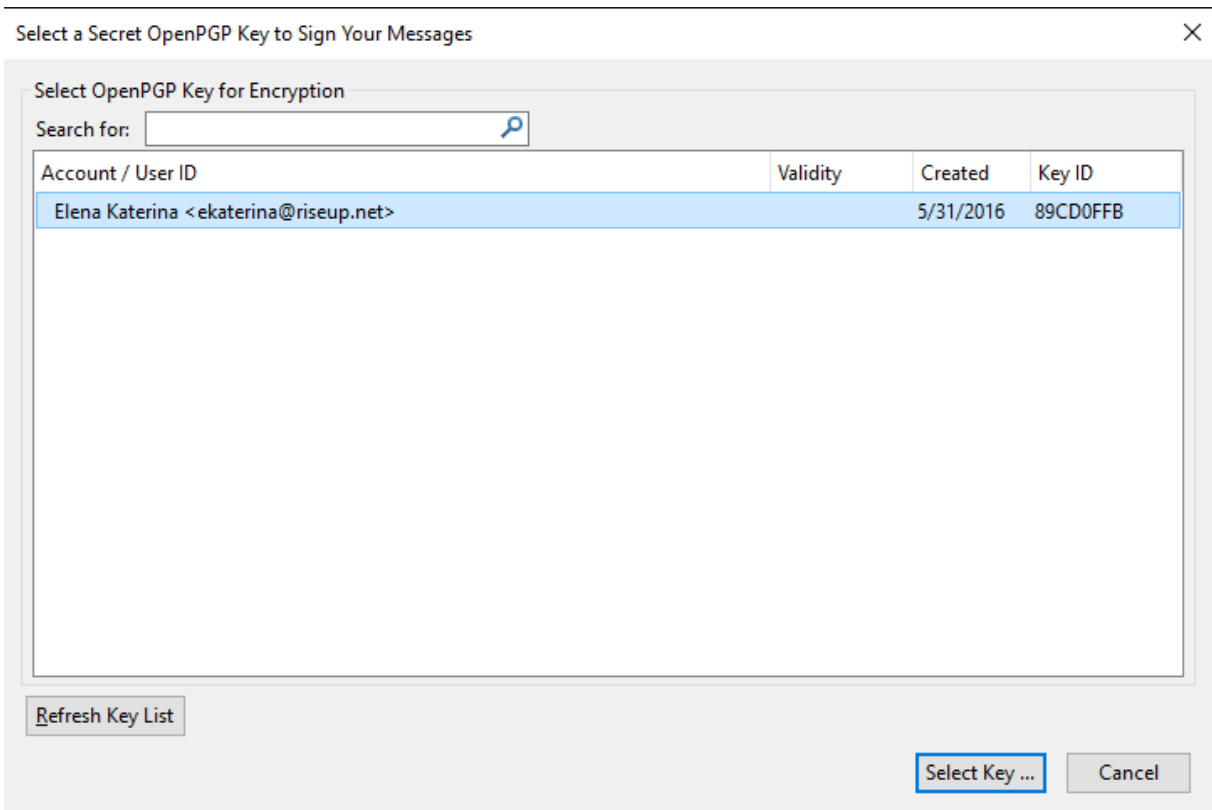


Figura 5: Elegir un par de claves para una cuenta de correo electrónico particular en Thunderbird

Paso 6. Haz clic en [Elegir claves...] para enlazar este *par de claves* con esta cuenta de correo electrónico y regresar a la pantalla de configuración de *OpenPGP Security*.

Abajo, recomendados dos configuraciones opcionales, no predeterminadas.

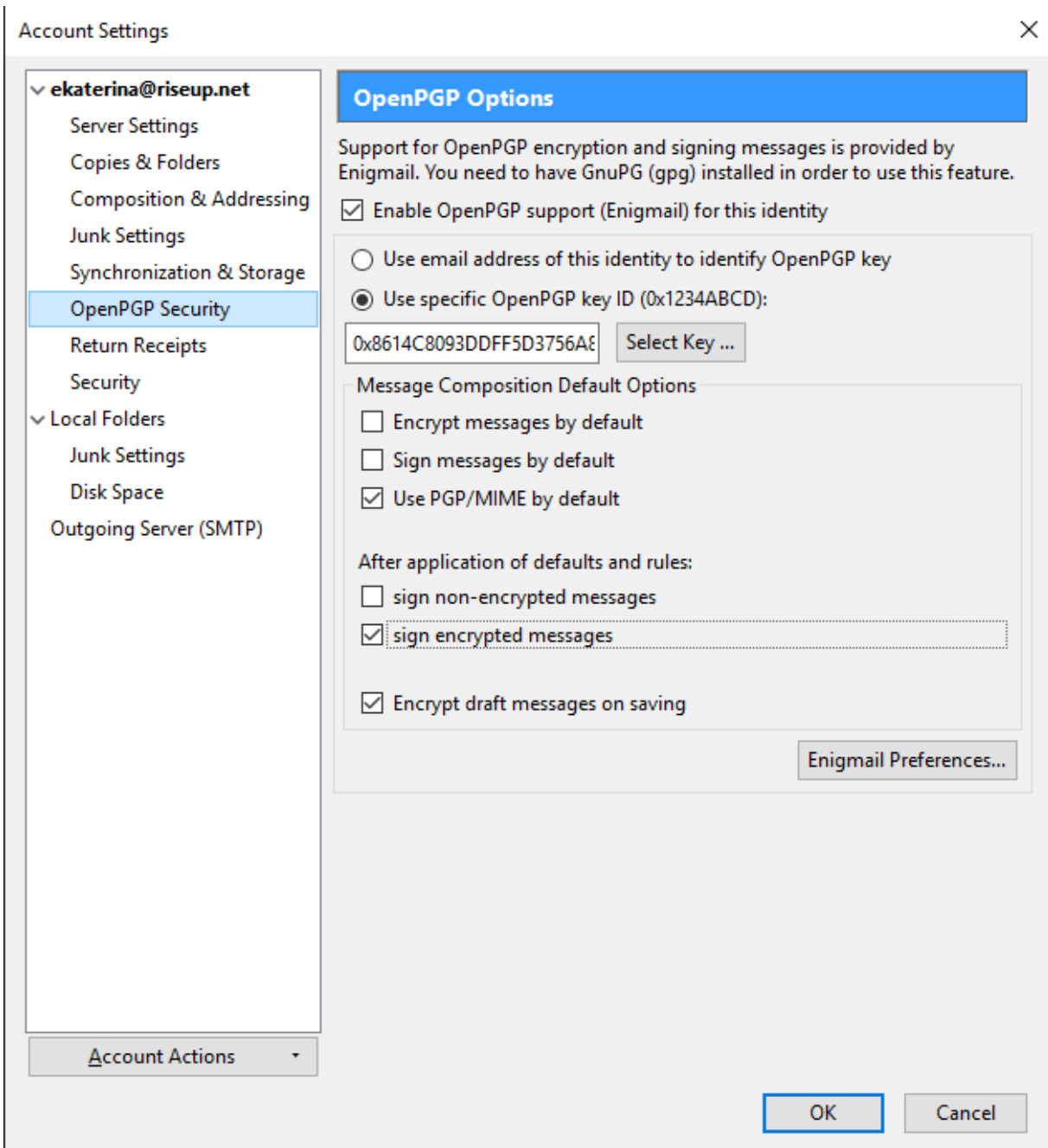


Figura 6: Configurar Enigmail para esta cuenta de correo electrónico

Paso 7. Marcar el recuadro [Usar PGP/MIME por defecto].

Con este recuadro marcado, Enigmail tiene mejor capacidad para encriptar adjuntos de correos electrónicos, incluidos los nombres de sus archivos.

Paso 8. Marca el recuadro [firmar mensajes encriptados].

Con este recuadro marcado, Enigmail firmará digitalmente todo correo electrónico encriptado enviado a ti a través de esta cuenta a menos que indiques específicamente que no lo haga. Los mensajes sin encriptar quedarán sin firma por defecto.

Paso 9. Haz clic en [OK] para regresar a Thunderbird.

4.2.3 VER Y ADMINISTRAR LAS PROPIEDADES DE TU CLAVE

Una vez que hayas generado tu *par de claves* de **GnuPG** y configurado tu cuenta de correo electrónico para que funcione con **Enigmail**, puedes ver y administrar las propiedades de tu *par de claves* siguiendo los pasos a continuación.

Paso 1. Haz clic en  y elige [Enigmail > Administración de claves].

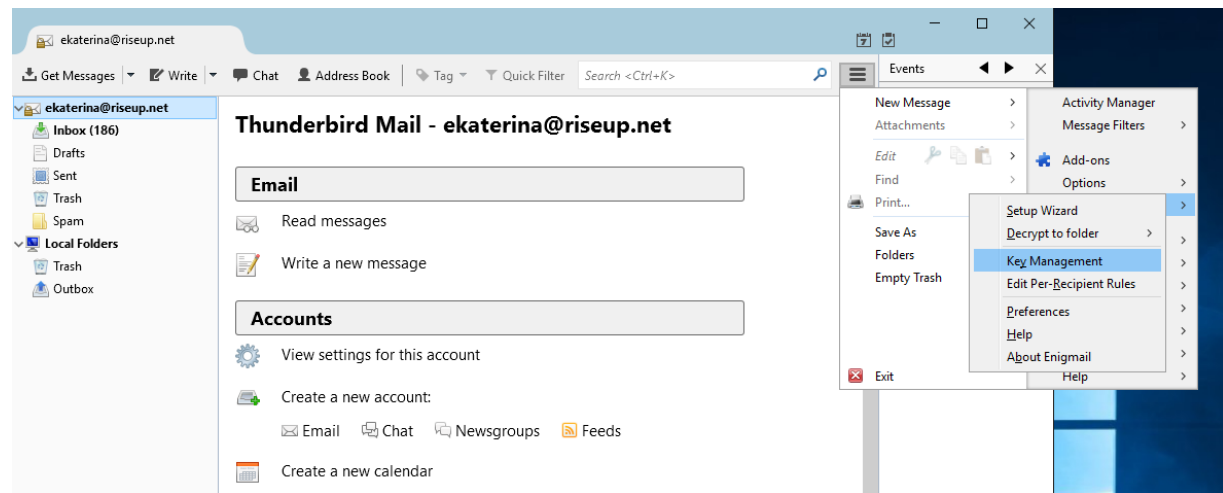


Figura 1: Abrir la pantalla de Administración de claves de Enigmail

Esto activará tu pantalla de Administración de claves de Enigmail.

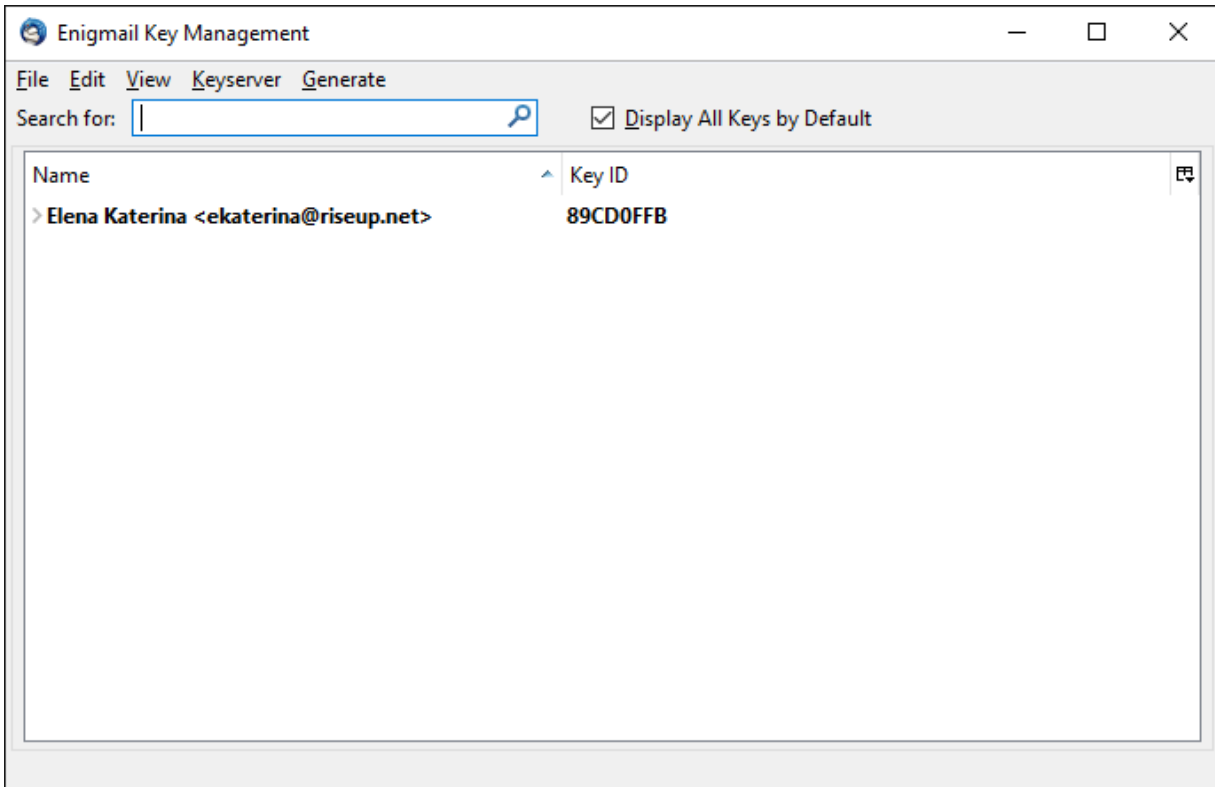


Figura 2: Pantalla de Administración de claves de Enigmail

Paso 2. Haz doble clic en el nombre de tu *par de claves* para ver o editar sus propiedades.

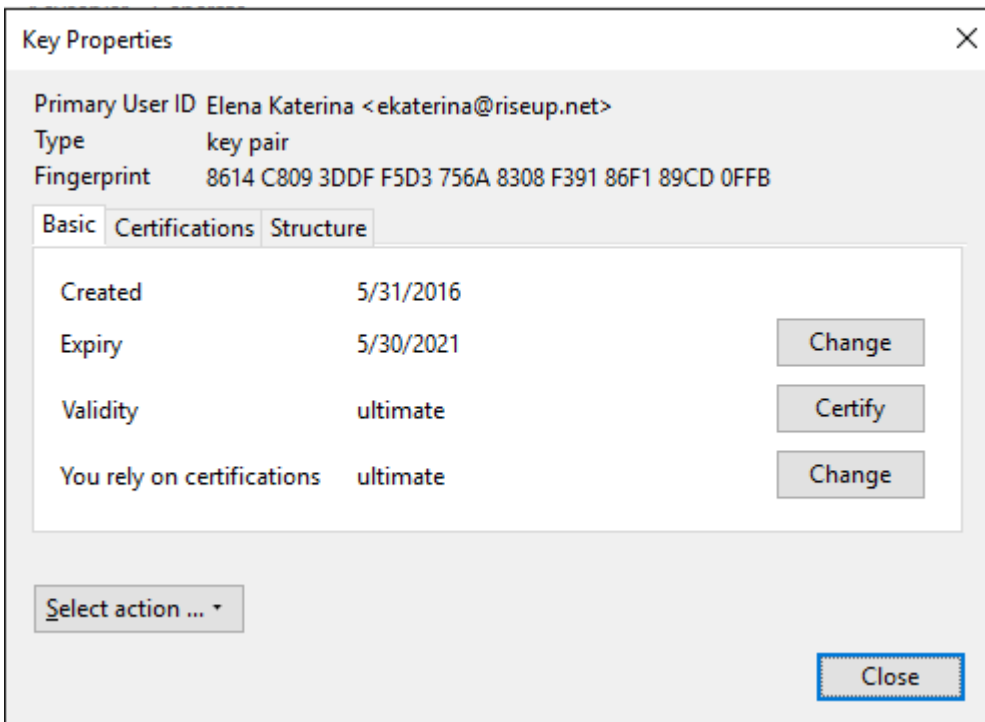


Figura 3: Propiedades de par de claves

La ventana de Propiedades de la clave muestra información importante tu *par de claves* de **GnuPG**:

- **Identificación de clave:** La *identificación de clave* que se muestra abajo para *ekaterina@riseup.net* es **0x89CD0FFB** (esto corresponde a los ocho últimos dígitos de la *huella digital de la clave* completa de abajo).
- **Huella digital de la clave:** La *huella digital de la clave* para el mismo *par de claves* es **8614 C809 3DDF F5D3 756A 8308 F391 86F1 89CD 0FFB**. Tu *huella digital de la clave* no es algo que debas mantener en secreto. En realidad, se debe compartir.
- **Fecha de expiración:** Este *par de claves* no funcionará después del 30 de mayo del 2021.

Antes de que otros puedan enviarte correo electrónico encriptado, deben tener una copia de tu *clave pública*. Puedes saber más sobre compartir claves en la [Sección 4.3](#). La *huella digital de tu clave* es una parte importante de cómo otros pueden estar seguros de que la clave que tienen es *realmente tuya*. Analizamos la *verificación de claves* en la [Sección 4.4](#).

(OPCIONAL) CAMBIAR LA FECHA DE EXPIRACIÓN DE UN PAR DE CLAVES

Si necesitas cambiar la fecha de expiración de tu *par de claves* de **GnuPG**, sigue los pasos a continuación. Esto es más útil como una manera de *extender* una fecha de expiración, a medida que se acerca, si necesitas más tiempo para generar un nuevo *par de claves* e informar a las personas con quienes te comunicas usando correo electrónico encriptado.

Paso 1. Haz clic en [Cambiar] al lado de la fecha de expiración de tu par de claves.

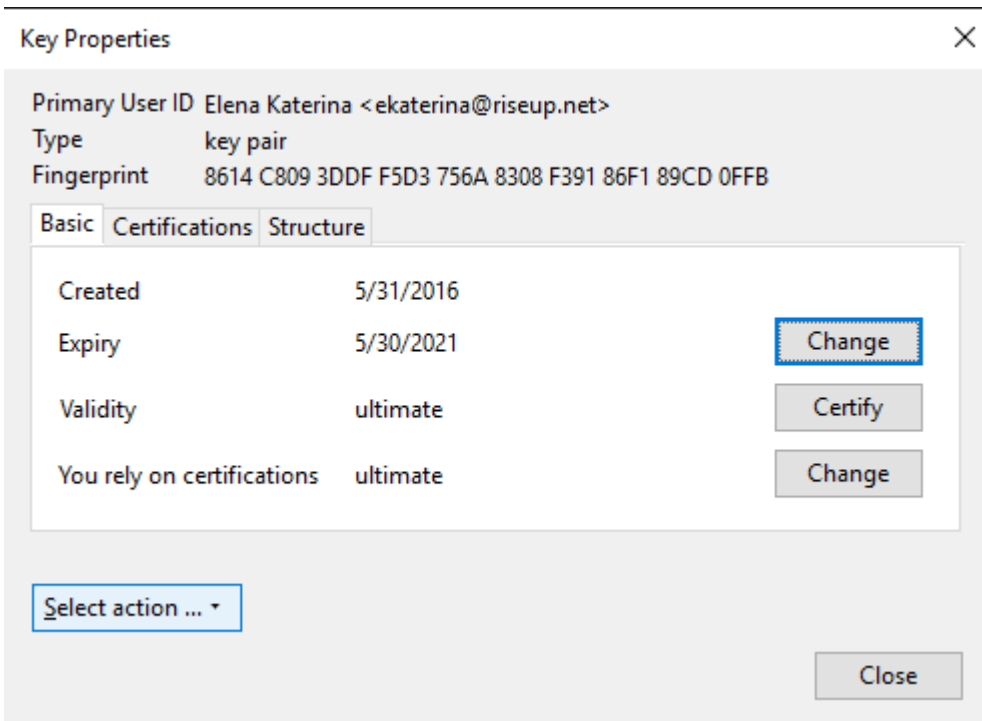


Figura 1: Cambiar la fecha de expiración de un par de claves

Esto activará la pantalla de *cambiar fecha de expiración* que se muestra abajo.

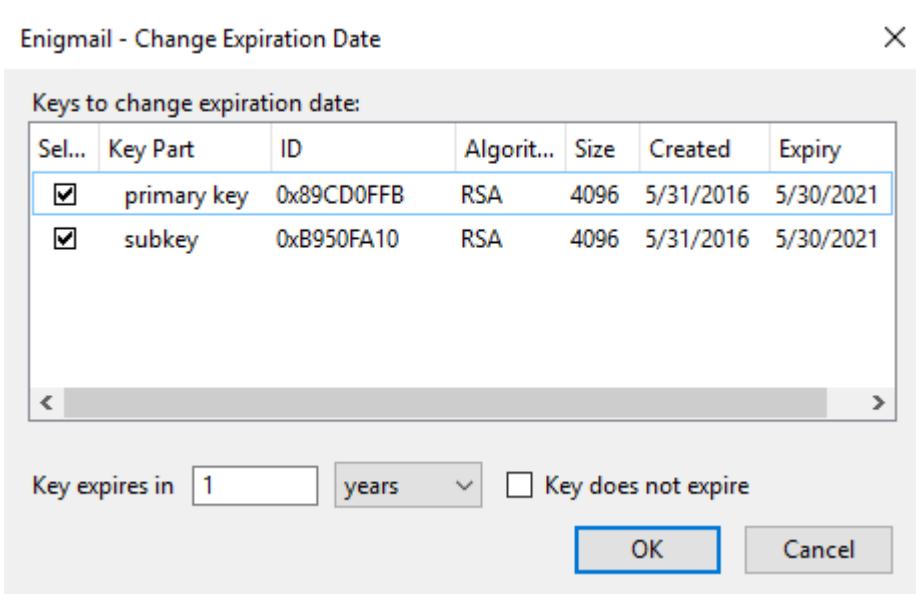


Figura 2: Pantalla de cambio de fecha de expiración de Enigmail

Nota: El número de años que se muestra en la parte de abajo de la pantalla

no necesariamente coincide con la fecha de expiración actual. Si haces clic en **[OK]** sin cambiar nada, puedes reducir temporalmente la duración de tu *par de claves*.

Paso 2. Escribe la cantidad de años, empezando desde hoy, que quisieras que este *par de claves* funcionara.

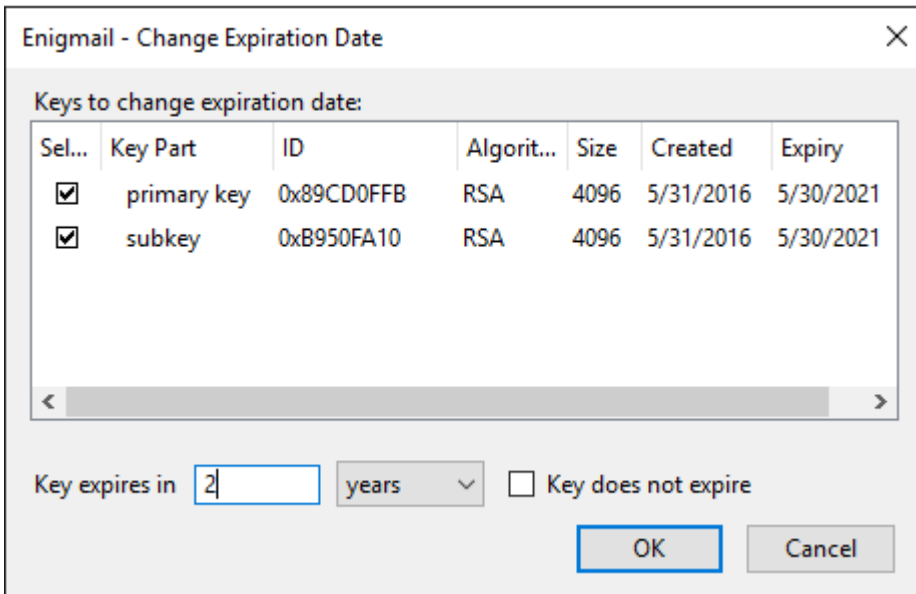


Figura 3: Cambiar la fecha de expiración de un par de claves de GnuPG

Paso 3. Haz clic en [OK] para escribir la contraseña de tu clave privada.

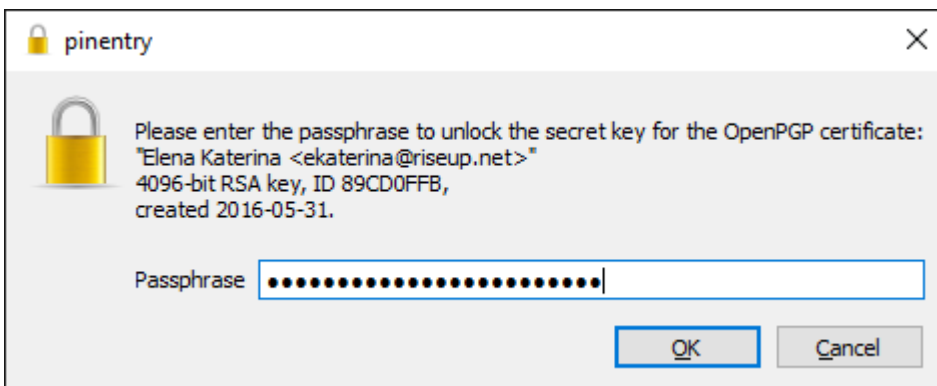


Figura 4: Escribir una contraseña para clave privada

Paso 4. Escribe tu contraseña.

Paso 5. Haz clic en [OK] para cambiar la fecha de expiración de tu *par de claves* de GnuPG.

(OPCIONAL) CAMBIAR LA CONTRASEÑA DE UNA CLAVE PRIVADA

Recomendamos cambiar tu contraseña de vez en cuando, solamente en caso de que haya sido puesta en peligro sin tu conocimiento. Si quieres cambiar la contraseña que protege tu clave privada, sigue los pasos a continuación.

Paso 1. Haz clic en [Elige acción...] y elige [Cambiar contraseña].

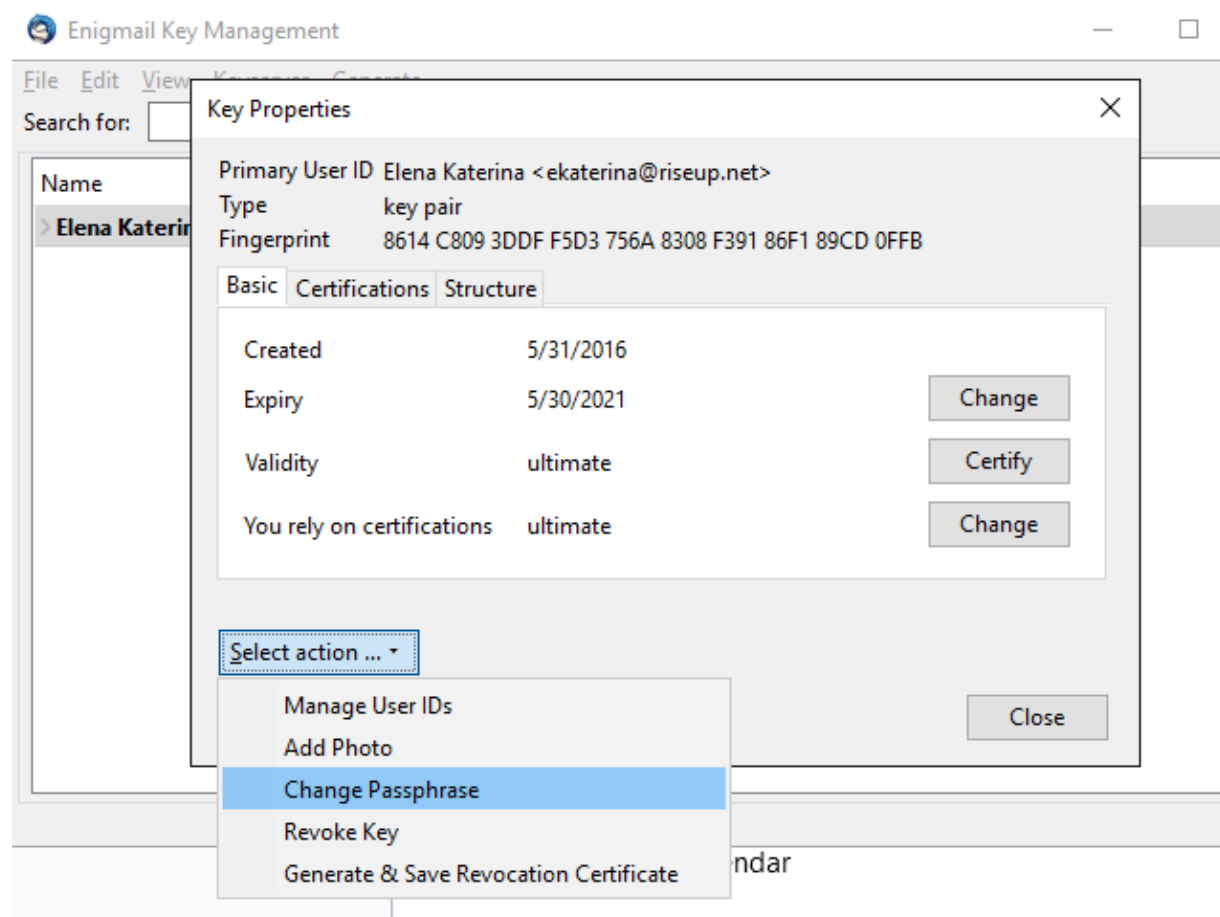


Figura 1: Cambiar una contraseña

Paso 2. Escribe la contraseña actual para tu clave privada.

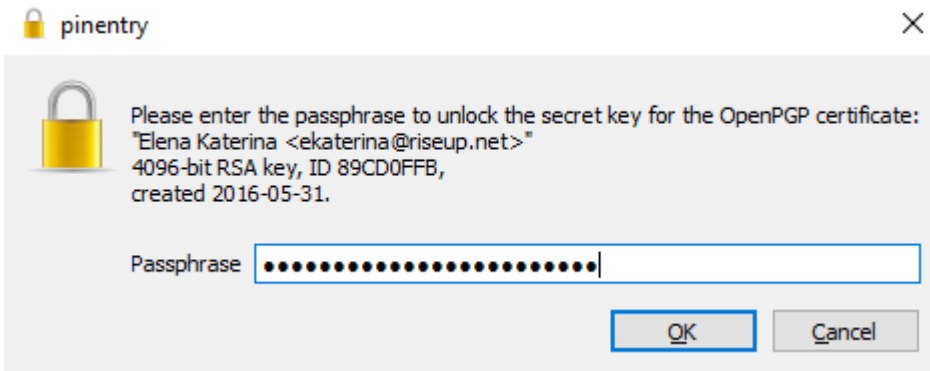


Figura 2: Escribir una contraseña para clave privada

Paso 3. Haz clic en [OK].

Paso 4. Escribe tu nueva contraseña y haz clic en [OK].

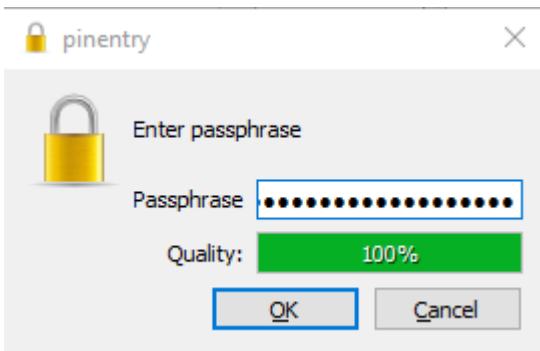


Figura 3: Escribir una nueva contraseña para clave privada

Paso 5. Vuelve a escribir tu nueva contraseña y haz clic en [OK].

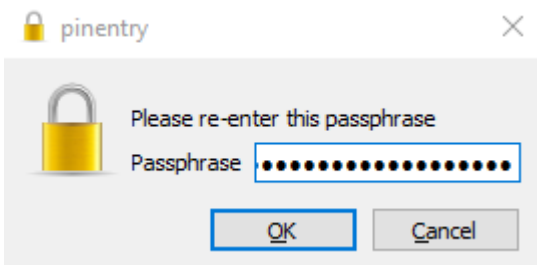


Figura 4: Volver a escribir la nueva contraseña para clave privada

Ya has cambiado la contraseña para tu clave privada.

4.3 INTERCAMBIAR CLAVES PÚBLICAS

Antes de que empiecen a enviarse correos electrónicos encriptados entre ustedes, tú y la personas con quienes te escribes deben intercambiar claves públicas. También debes confirmar la validez de cualquier clave que hayas recibido y confirmar que realmente le pertenece a la persona que crees que la envió.

4.3.1 ENVIAR TU CLAVE PÚBLICA COMO ADJUNTO DE CORREO ELECTRÓNICO

Para enviar una clave pública usando Enigmail, tú y la persona con quien te escribes deberán llevar a cabo los siguientes pasos:

Paso 1. Abre Thunderbird y **haz clic** en **[Escribir]** para escribir un correo electrónico.

Paso 2. Elige **[Enigmail > Adjuntar clave pública...]**. (Alternativamente, **haz clic** en el botón de **[Adjuntar mi clave pública]** encima de tu dirección de correo electrónico, omite los pasos siguientes y anda directamente al paso 4.)

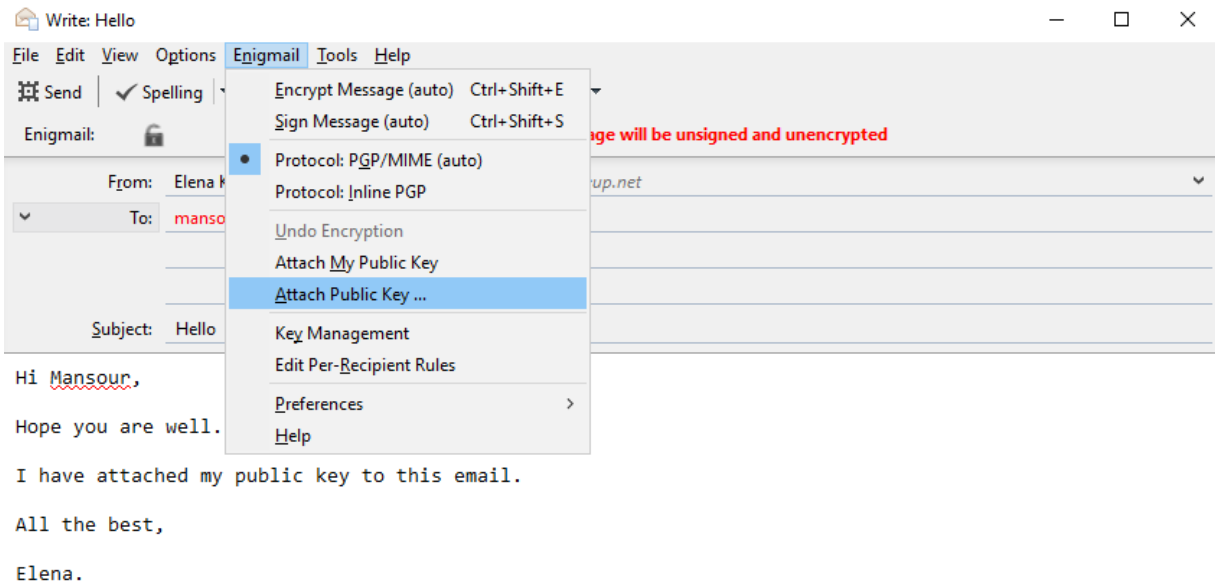


Figura 1: Adjuntar una clave pública

Paso 3. Elige la clave que quisieras enviar (por lo general, la que está asociada con la cuenta de correo electrónico que estás usando actualmente).

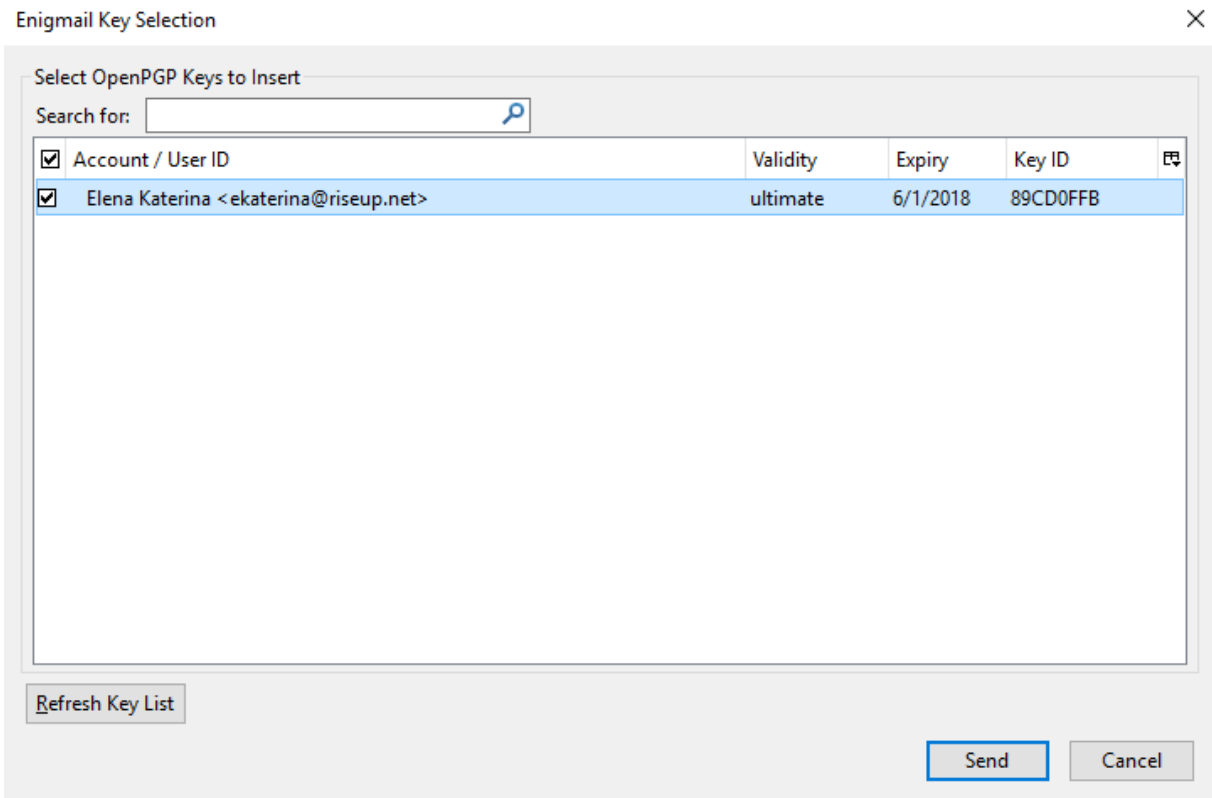


Figura 2: Elegir qué clave pública adjuntar

Paso 4. Haz clic en [Enviar]. Tu clave no aparecerá como adjunto hasta justo antes de que se envíe el correo electrónico.

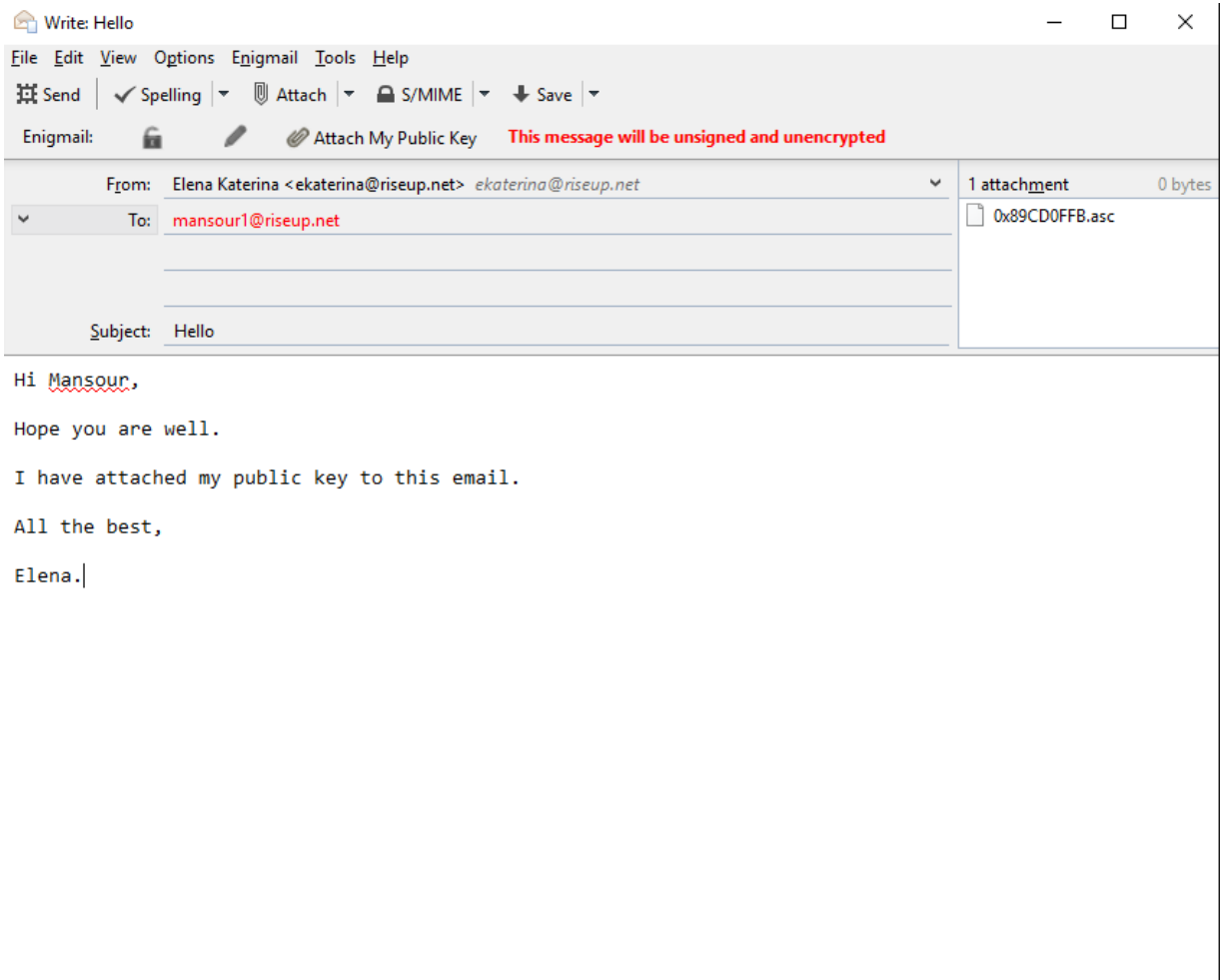


Figura 3: Clave pública adjunta y a punto de ser enviada

Paso 5. Escribe tu contraseña de GnuPG y **presiona Aceptar** si así se indica.

4.3.2 IMPORTAR UNA CLAVE PÚBLICA ADJUNTA A UN CORREO ELECTRÓNICO

Tú y la persona con quien te escribes deben seguir los pasos a continuación para importar las claves públicas del otro.

Una clave pública adjunta debe estar visible en la esquina inferior izquierda del correo electrónico en el que se envió:



Figura 1: Clave pública adjunta a un correo electrónico

Paso 1. Haz clic derecho en el adjunto y elige [Importar clave de OpenPGP] para importar la *clave pública* de la persona con quien te escribes.

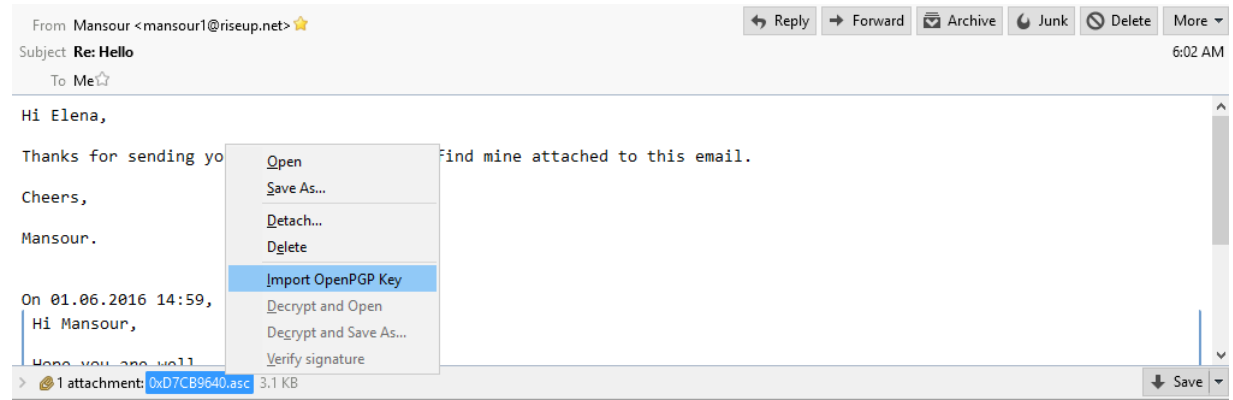


Figura 2: Importar una clave de OpenPGP

Paso 2. Haz clic en [Sí] para importar la clave pública de la persona con quien te escribes.

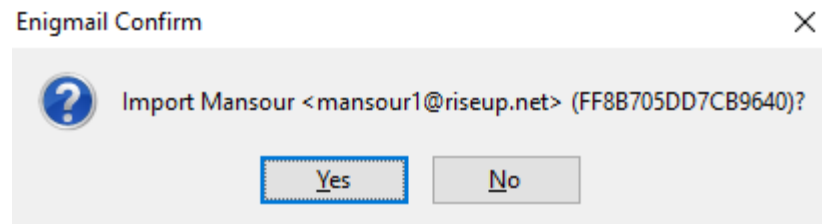


Figura 3: Ventana de confirmación de Enigmail

Paso 3. Haz clic en [OK] para cerrar la ventana que dice que la(s) *clave(s)* se importaron satisfactoriamente.

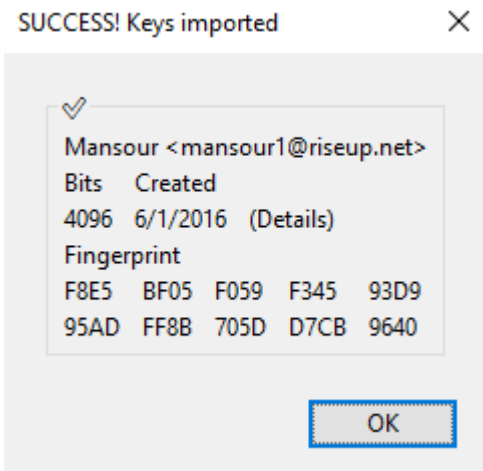


Figura 4: Claves pública importada satisfactoriamente

Paso 4. Haz clic en  y elige [Enigmail > Administración de claves].

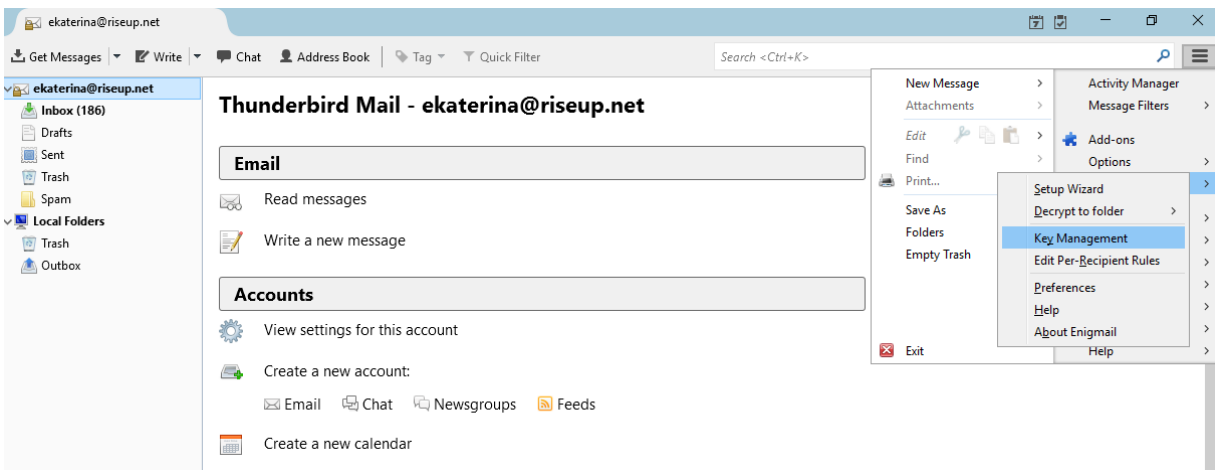


Figura 5: Abrir la ventana de Administración de claves de Enigmail

Ahora debes poder ver la clave pública de la persona con quien te escribes:

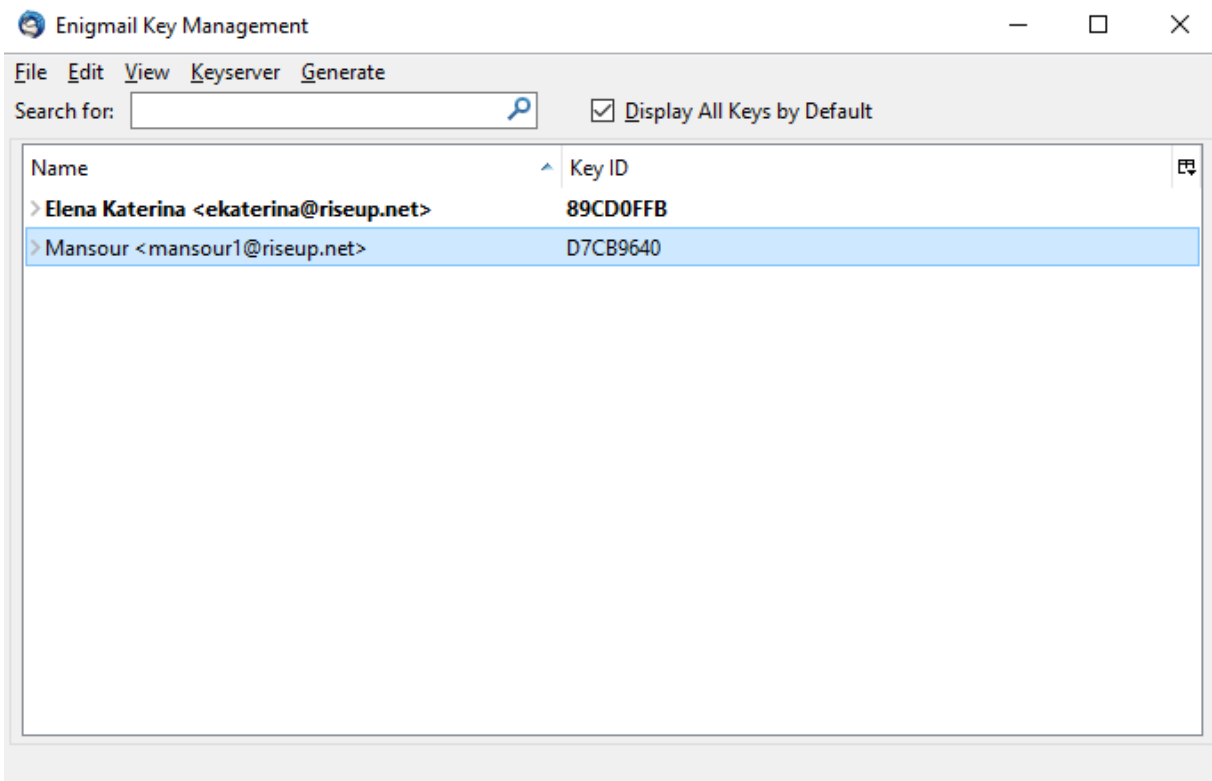


Figura 6: Una nueva clave pública mostrada en la pantalla de Administración de claves de Enigmail

4.4 VALIDAR Y FIRMAR CLAVES PÚBLICAS

Ahora debes verificar que la clave que has importado realmente pertenece a la persona que crees que te la envió. Este es un proceso que tú (y las personas con quienes te escribes) deben completar para cada clave pública que reciban. Cuando verifiques la clave, la *firmarás* para que GnuPG sepa que es válida.

4.4.1 VALIDAR LA CLAVE PÚBLICA DE OTRA PERSONA

Para validar la clave pública de la persona con quien te escribes, contáctala usando un medio de comunicación que te permita estar absolutamente seguro de que estás hablando con la persona correcta. Las reuniones en persona son mejores, pero las conferencias de voz y video son aceptables si confías en reconocer la voz o el aspecto de la otra persona. *Esta*

conversación no tiene que ser confidencial, en tanto te abstengas de discutir temas delicados. Vas a intercambiar huellas digitales de *claves públicas* que no necesitan mantenerse en secreto.

Tú y la persona con quien te escribes deben verificar las *huellas digitales* de las claves públicas que han intercambiado. Una *huella digital* es una serie única de números y letras que identifica un *par de claves* de *GnuPG*. Puedes usar la pantalla de *Administración de claves* de **Enigmail** para ver la *huella digital* de los *pares de claves* que has generado y de las *claves públicas* que has importado.

Para ver la *huella digital* de un *par de claves* particular, sigue los pasos a continuación.

Paso 1. Haz clic en  y elige [Enigmail > Administración de claves].

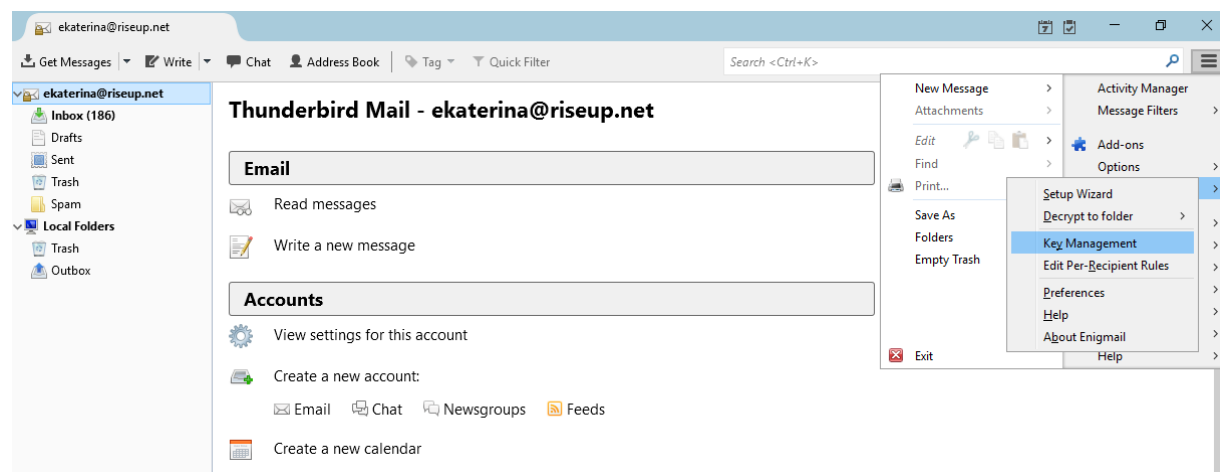


Figura 1: Abrir la Ventana de administración de claves de Enigmail

Paso 2. Haz doble clic en un *par de claves* para abrir la ventana de *Propiedades de claves* de **Enigmail**.

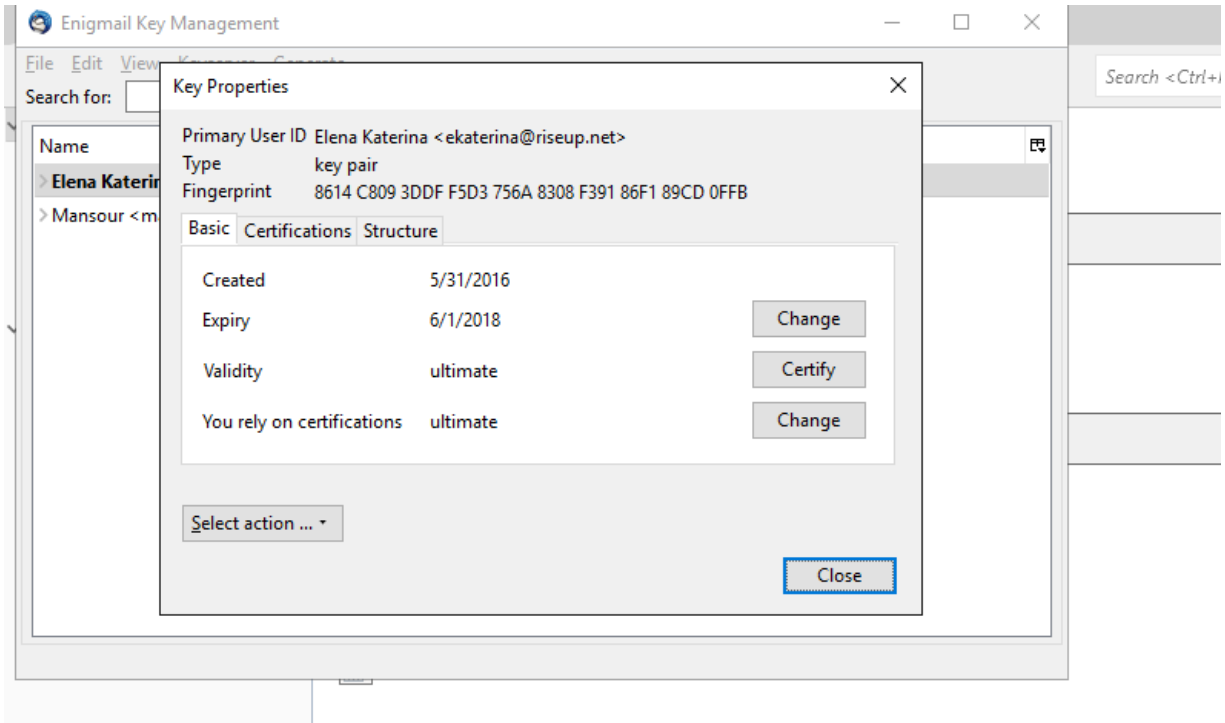


Figura 2: Pantalla de Propiedades de claves de Enigmail

En la ventana *Propiedades de claves*, podrás ver la huella digital del *par de claves* elegido. Por ejemplo. la huella digital de *ekaterina@riseup.net* es **8614 C809 3DDF F5D3 756A 8303 F391 86F1 89CD 0FFB**.

La persona con quien te escribes debe realizar también estos pasos. Entonces, para verificar huellas digitales:

1. Lee la huella digital de tu par de claves a la persona con quien te escribes
2. Hazle que verifique que las huellas digitales que tiene para tu clave pública coincidan con las que acabas de darle
3. Haz que la persona con quien te escribes te lea tu huella digital para *su* par de claves
4. Verifica que la huella digital que *tú* tienes para su clave pública coincida con la que te acaba de dar

Si las huellas digitales no coinciden, intercambien claves públicas de nuevo y repitan el proceso.

Nota: Como las propias huellas digitales de la claves no son sensibles, fácilmente puedes escribir la huella digital que te lea la persona con quien te escribes. Después, cuando tengas más tiempo, puedes verificar que coincida con la huella digital que *tú* tienes para su clave pública usando la pantalla de *Administración de claves* de Enigmail (también es por eso que algunas personas imprimen sus huellas digitales GnuPG en sus tarjetas de presentación).

4.4.2 FIRMAR LA CLAVE PÚBLICA DE OTRA PERSONA

Una vez que hayas verificado la clave de alguien con quien te escribes, debes *firmarla*. Esto le dirá a Enigmail que recuerde que consideras válida esta clave.

Importante: Si firmas la clave pública de otra persona y haces que la *copia firmada* de *su* clave esté disponible públicamente, se puede dar a conocer fácilmente que intercambias información delicada con esa persona. Para evitar que eso ocurra por accidente, **marca siempre el recuadro *Firma local* cuando firmes la clave pública de una persona con quien te escribas.**

Puedes firmar una clave pública validada siguiendo los pasos a continuación.

Paso 1. Haz clic en  y elige [Enigmail > Administración de claves].

Paso 2. Haz clic derecho en la clave pública que quieres firmar y elige [Firmar clave].

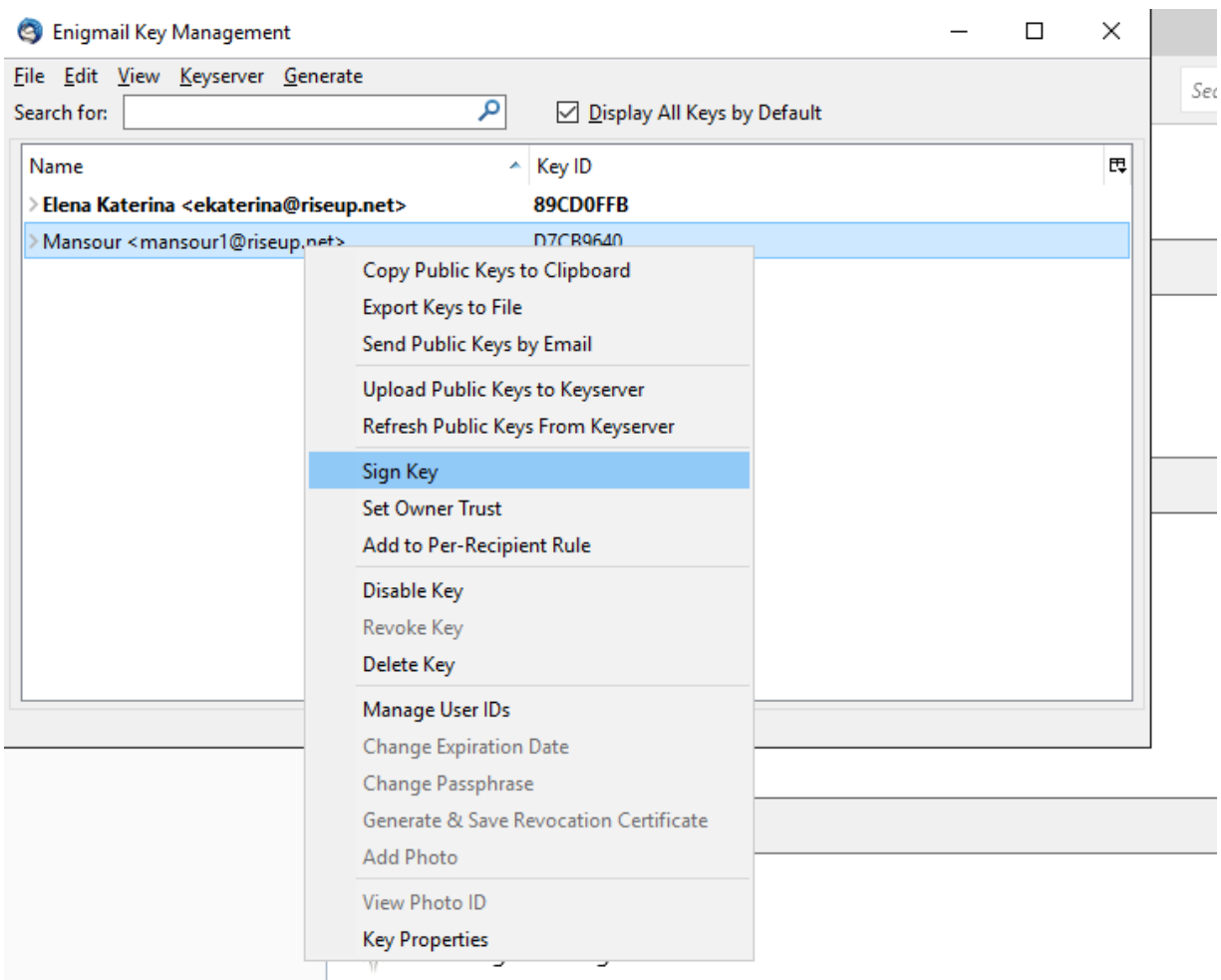


Figura 1: Firmar la clave pública de otra persona

Paso 3. Asegúrate de que tu *par de claves* esté elegido al lado de *Clave para firmar*.

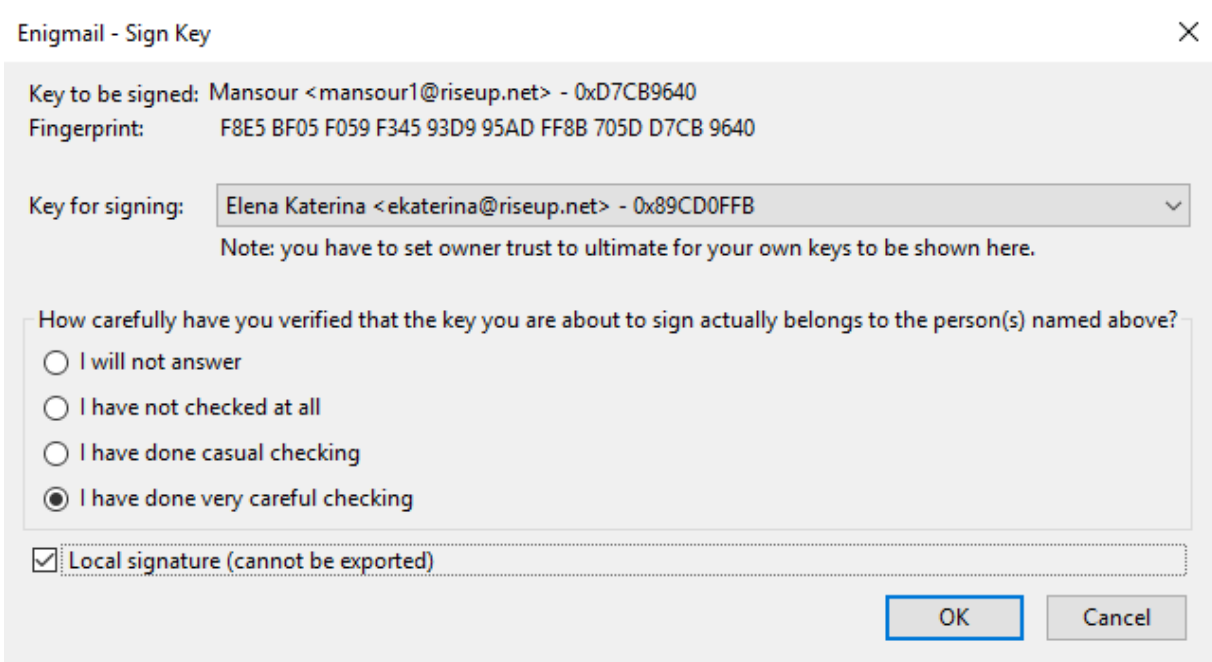


Figura 2: Pantalla de Firmar clave de Enigmail

Paso 4. Haz clic en [He hecho una revisión muy cuidadosa].

Nota: Otras opciones (como *No he revisado para nada*) pueden no permitirte enviar mensajes encriptados al dueño de esta clave. Y, debido a un fallo en **Enigmail**, puede ser difícil cambiar esta configuración después. Por tanto, recomendamos que siempre elijas *He hecho una revisión muy cuidadosa* al firmar en la *clave pública* de la persona con quien te escribes.

Paso 5. Marca el recuadro [Firma local (no puede ser exportada)].

Importante: A menos que confíes mucho en **GnuPG** – y sepas con certeza que el dueño de esta *clave pública* quiere que su firma sea pública – debes marcar este recuadro.

Paso 6. Haz clic en [OK].

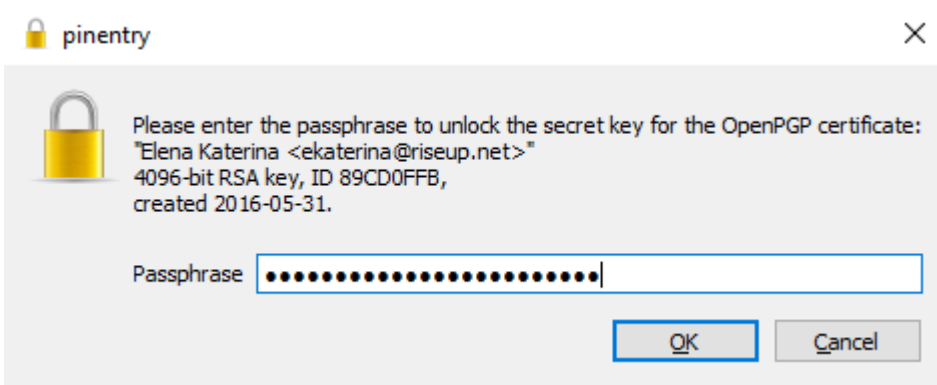


Figura 3: Escribir la contraseña para tu clave privada para firmar la clave pública de otra persona

Paso 7. Escribe la contraseña de tu clave privada.

Paso 8. Haz clic en **[OK]** para firmar esta clave pública. Esto le dirá a Enigmail que has verificado la identidad de su propietario, lo que te permitirá enviarle correo electrónico encriptado.

4.5 ENCRIPITAR Y DESENCRIPTAR MENSAJES DE CORREO ELECTRÓNICO

GnuPG solamente protege el **contenido** de correo electrónico y adjuntos que encriptes. La siguiente información nunca está encriptada:

- La línea de *Asunto*
- La dirección de correo electrónico del remitente
- Las direcciones de correo electrónico de los destinatarios
- Todo nombre real que se pueda asociar con remitentes y destinatarios (Elena S. Katerina <ekaterina@riseup.net>, por ejemplo)

Además, si configuras Enigmail para usar *Inline PGP* en lugar de *PGP/MIME*, los nombres de archivos de los adjuntos que envíes quedarán sin encriptar.

Por lo tanto, es importante escoger con cuidado las líneas del asunto, evalúa crear una clave de GnuPG al menos para una cuenta de correo

electrónico que no incluya tu nombre real y usa siempre *PGP/MIME*.

Finalmente, cuando envíes correo electrónico encriptado, una copia — encriptada a *tu* clave pública — se colocará en tu carpeta *Correo enviado*.

4.5.1 ENVAIR CORREO ELECTRÓNICO ENCRIPTADO

Una vez que tú y la persona con quien te escribes hayan importado, validado y firmado satisfactoriamente las claves públicas del otro, pueden empezar a intercambiar mensajes encriptados.

Puedes encriptar el contenido de tu mensajes de correo electrónico siguiendo los pasos a continuación:

Paso 1. En Thunderbird, **haz clic** en **[Escribir]** y redacta un correo electrónico a un destinatario para quien hayas firmado una *clave publica*.

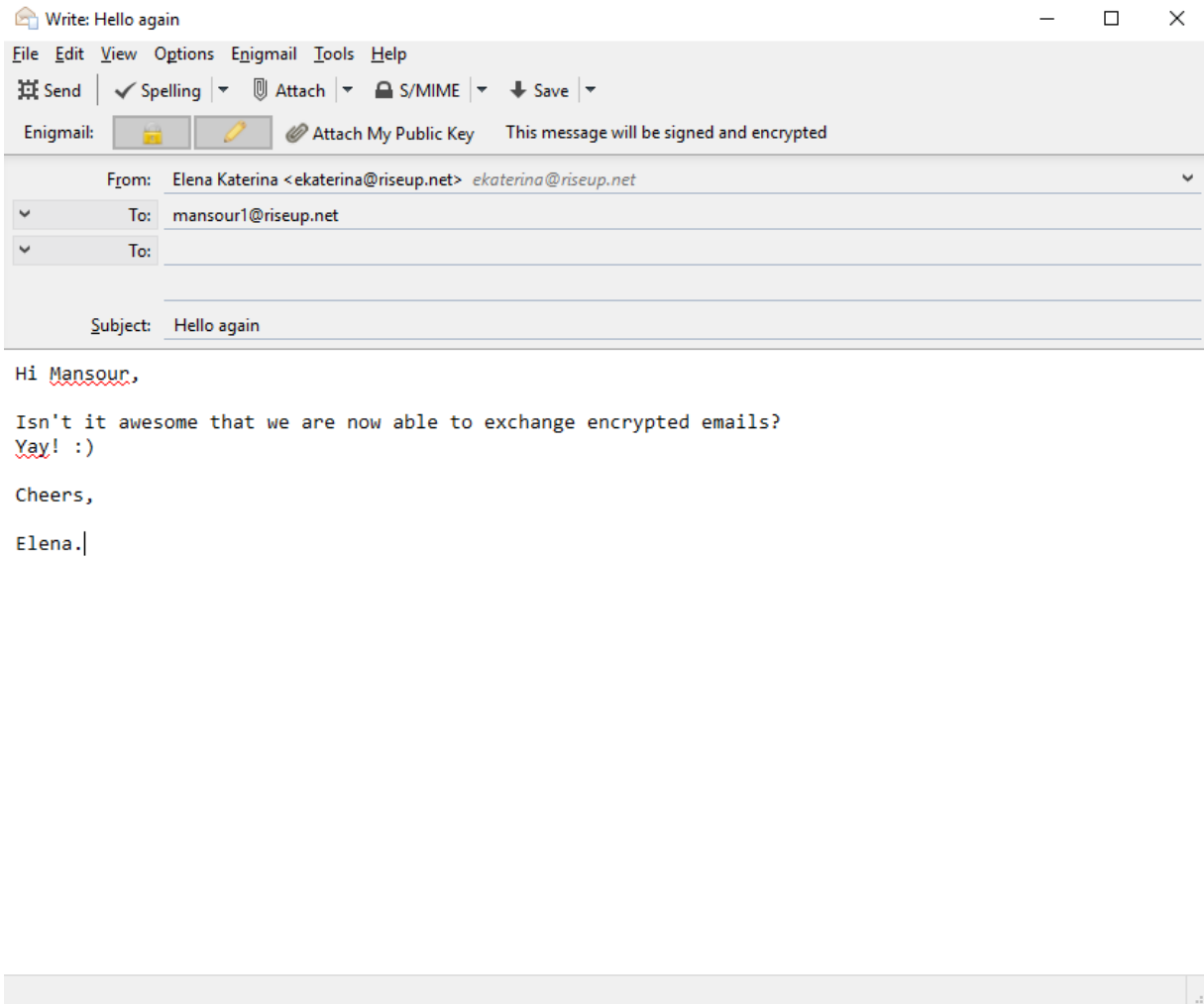


Figura 1: Ventana de Redactar de Thunderbird

Importante: El botón del candado (que indica que tu mensaje estará encriptado) y el botón del lápiz (que indica que tu mensaje estará firmado) se deben encender en cuanto hayas escrito una dirección de correo electrónico para el que tengas una clave pública válida y firmada. También debes ver **"Este mensaje estará firmado y encriptado"** hacia la esquina superior derecha de la ventana. Esto es porque:

- Por defecto, Enigmail encripta automáticamente el correo electrónico para personas con quienes te escribas para quienes tengas una clave pública válida
- Hemos activado **firmar mensajes encriptados**, debajo de

[Configuraciones de cuenta > Seguridad de OpenPGP] en una sección anterior.

Puedes elegir *no* encriptar ni firmar un mensaje inhabilitando los botones del candado o el lápiz antes de hacer clic en **[Enviar]** (también puedes configurar Thunderbird para enviar correo electrónico no encriptado por defecto. Esta opción está debajo de las Configuraciones manuales de encriptación en la pestaña de Enviar del menú de preferencias de Enigmail).

Paso 2. Haz clic en Enigmail en la barra de menú de la ventana Redactar.

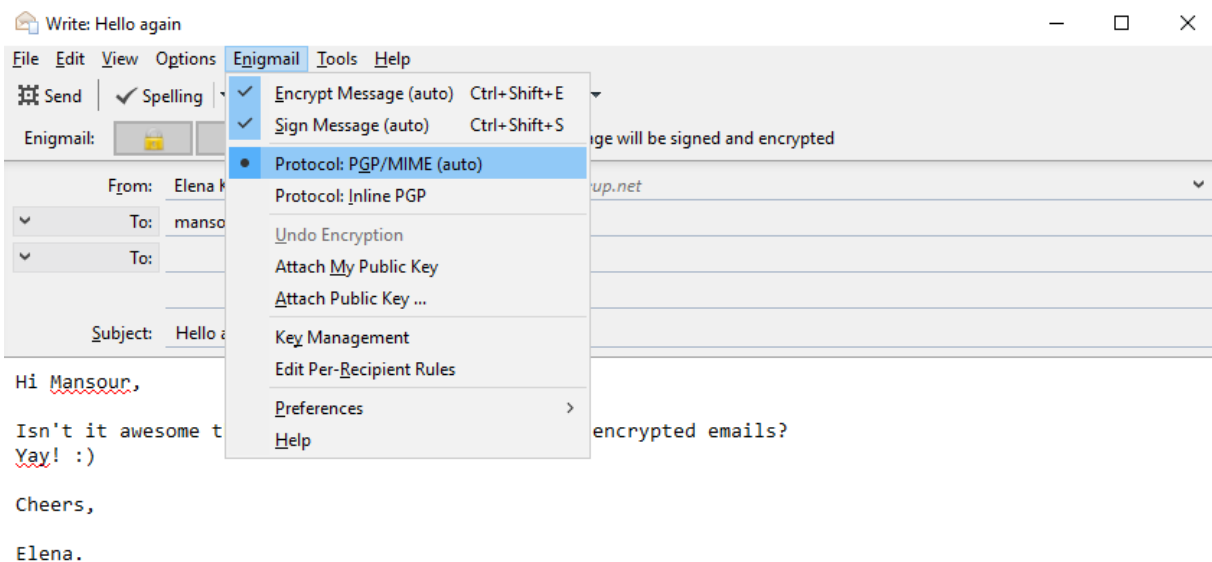


Figura 2: Habilitar encriptación y firma

Paso 3. Marca el recuadro de Encriptar mensaje.

Paso 4. Marca el recuadro Firmar mensaje.

Cuando hayas escrito una dirección en **Para: para quien tienes una clave pública verificada**, deberá aparecer el siguiente mensaje en la ventana superior derecha de la ventana:

This message will be signed and encrypted

Figura 3: Enigmail te dice que está listo para encriptar y firmar un mensaje

Paso 5. Haz clic en [Enviar].

Paso 6. Escribe la contraseña de tu clave privada.

Paso 7. Haz clic en [OK] para enviar tu mensaje (encriptado y firmado).

4.5.2 DESENCRIPTAR UN CORREO ELECTRÓNICO DE OTRA PERSONA

Cuando haces clic en un mensaje encriptado, Enigmail te pedirá la contraseña de tu clave privada para que puede desenscriptar el mensaje.

Escribe tu contraseña y **haz clic** en **[Abrir]**.

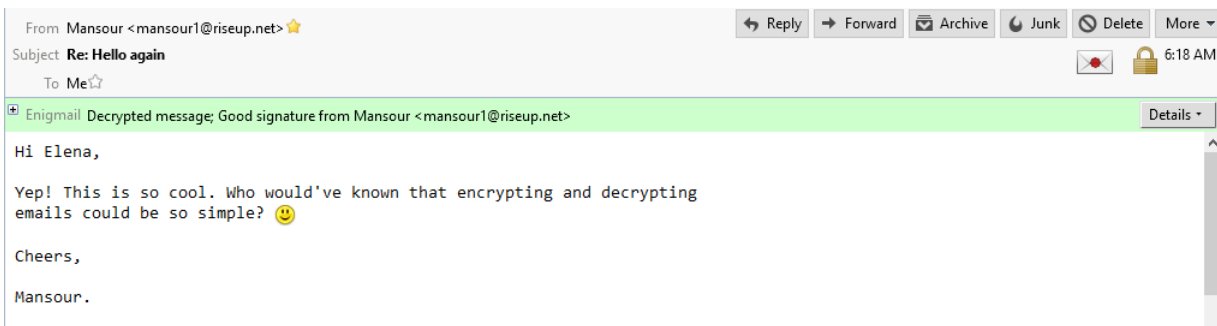


Figura 1: Mensaje desenscriptado con una firma verificada

Enigmail mostrará algo de información en la parte de arriba del mensaje. En la figura de arriba, por ejemplo, "**Mensaje desenscriptado; Firma buena de Mansour**" te dice:

- El mensaje fue encriptado usando tu clave pública (lo que puede hacer cualquiera)
- Lo has desenscriptado satisfactoriamente
- Lo firmó alguien con la clave privada que corresponde a la clave pública de *mansour@riseup.net* que has importado
- Has firmado esa clave pública de *mansour@riseup.net*, ojalá despues de haber verificado que pertenece al *verdadero* Mansour.

PREGUNTAS FRECUENTES

P: ¿Qué pasa si solamente instalo Enigmail y no GnuPG?

R: Eso es simple, realmente. Enigmail no va a funcionar. Después de todo, es el software de GnuPG el que brinda el motor de encriptación que usa Enigmail.

P: ¿Cuántas cuentas de correo electrónico puedo configurar en Thunderbird?

R: ¡Tantas como quieras! Thunderbird es un administrador de correo electrónico, ¡y puede administrar fácilmente 20 o más cuentas de correo electrónico!

P: Mi amigo tiene una cuenta de Gmail. ¿Debo convencerlo de instalar Thunderbird, Enigmail y GnuPG?

R: Sería lo ideal. Solamente asegúrate de que configure todas estos ajustes de seguridad en la misma manera exacta que has hecho tú. ¡Entonces los dos tendrán una forma extremadamente efectiva de comunicarse con privacidad y seguridad!

P: Recuérdame otra vez, ¿qué partes de un mensaje de correo electrónico encripta Enigmail?

R: Enigmail solamente encripta el *contenido* de los mensajes. Las líneas de Asunto no estarán encriptadas, ni las direcciones de correo electrónico de remitente y destinatario (ni los nombres asociados con esas direcciones). Así que escoge tus líneas de Asunto con cuidado y evalúa crear una clave GnuPG para al menos una cuenta de correo electrónico que no incluya tu nombre real.

P: Sigo sin entender el objetivo de firmar digitalmente mis mensajes.

R: Una firma digital prueba que eres el verdadero remitente de un mensaje particular y que el mensaje no ha sido adulterado en su camino al

destinatario previsto. Considéralo como el equivalente electrónico del sello de un sobre que contiene una carta muy importante.

Este trabajo está licenciado bajo la licencia Creative Commons Attribution-Share Alike 3.0 Unported License. (<http://creativecommons.org/licenses/by-sa/3.0/>)

Security-in-a-Box es un proyecto de Tactical Technology Collective (<https://tacticaltech.org>) and Front Line Defenders (<https://www.frontlinedefenders.org/>)